

Security in Practice: Examining the Collaborative Management of Sensitive Information  
in Childcare Centers and Physicians' Offices

Laurian C. Vega

Dissertation submitted to the faculty of the Virginia Polytechnic Institute and State  
University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy  
In  
Computer Science

Steve Harrison  
Dennis Kafura  
D. Scott McCrickard  
Enid Montague  
Deborah Tatar

February 28th, 2010  
Blacksburg, Virginia

Keywords: Security, Trust, Privacy, Usable Security,  
Computer Supported Collaborative Work

# Security in Practice: Examining the Collaborative Management of Personal Sensitive Information in Childcare Centers and Physician's Offices

Laurian C. Vega

## ABSTRACT

Traditionally, security has been conceptualized as rules, locks, and passwords. More recently, security research has explored how people interact in secure (or insecure) ways in part of a larger socio-technical system. Socio-technical systems are comprised of people, technology, relationships, and interactions that work together to create safe praxis. Because information systems are not just technical, but also social, the scope of privacy and security concerns must include social and technical factors. Clearly, computer security is enhanced by developments in the technical arena, where researchers are building ever more secure and robust systems to guard the privacy and confidentiality of information. However, when the definition of security is broadened to encompass both human and technical mechanisms, how security is managed with and through the day-to-day social work practices becomes increasingly important.

In this dissertation I focus on how sensitive information is collaboratively managed in socio-technical systems by examining two domains: childcare centers and physicians' offices. In childcare centers, workers manage the enrolled children and also the enrolled child's personal information. In physicians' offices, workers manage the patients' health along with the patients' health information. My dissertation presents results from interviews and observations of these locations. The data collected consists of observation notes, interview transcriptions, pictures, and forms. The researchers identified breakdowns related to security and privacy. Using Activity Theory to first structure, categorize, and analyze the observed breakdowns, I used phenomenological methods to understand the context and experience of security and privacy.

The outcomes from this work are three themes, along with corresponding future scenarios. The themes discussed are security embodiment, communities of security, and zones of ambiguity. Those themes extend the literature in the areas of usable security, human-computer interaction, and trust. The presentation will use future scenarios to examine the complexity of developing secure systems for the real world.

## Acknowledgements

I would like to thank many people who have helped me through the completion of this dissertation. The first is my advisor, Steve Harrison, who is captivating, honest, and the true embodiment of a mentor. In combination with the mentorship of my advisor, I am blessed to work with dynamic and intelligent committee members Dr. Dennis Kafura, Dr. D. Scott McCrickard, Dr. Enid Montague, and Dr. Deborah Tatar. I would also like to thank the Computer Science Department at Virginia Tech and ADVANCE NSF for funding my time at Virginia Tech. Peggy Layne, who worked with me at ADVANCE was a brilliant and insightful mentor. Additionally the mentorship of Victoria Bellotti, Oliver Brdiczka, Tara Matthews, and Tom Moran was instrumental to me during my internships, and their continued advice is invaluable.

This work was not completed in a vacuum. I worked with many brilliant students who broadened the value of the work: Laura Agnich, Monika Akbar, Aubrey Baker, Stacy Branham, Tom Dehart, Zalia Shams, and Edgardo Vega. Working with each of these students has been a gift that went much further than just completing work that needed to be done. Working with them expanded the value of the work. I appreciated each and every minute they spent with the data and (more important) with me.

I am thankful for and would like to acknowledge many others who helped me along the way: my father, Richard Hobby, who proofed many of my papers; my friends and family for late night phone calls; and my colleagues for bouncing ideas with me. This includes, but is not limited to Julia Hobby, Rich Hobby, Laura Harty, Elaine Hobby, Jason Lee, Shahtab Wahid, Tejinder Judge, Rishi Pande, Ross Goddard, Bobby Beaton, Sarah Peck, Kim Gausepohl, Kelly Meredith, Michael Evans, Jamika Burge, Manas Tungare, Ben Congleton, Pardha Pyla, Manuel Perez, Megan Beavers, Jocelyn Casto, Uma Murthy, Mara de Silva, Jon Howarth, Theresa Blanchard-Klunk, Sirong Lin, Joon Lee, Susan Wyche, Promita Chakraborty, Michael Stewart, the Garcoskis, Ben Hanrahan, Yeong-Tay Sun, Caitlin Sadowski, Alexandra Holloway, and Rex Hartson.

I am beyond grateful to all of my participants who were not paid to participate in the project. The people who participated in my study were generous with their time in a way that I can never repay.

Cameron Vega, my son, thank you for reorienting my life.

There are many neglected people and groups that are involved in the completion of a Ph.D. that I would like to acknowledge. I would like to thank Meg Kurdziolek for starting a dissertation writing group. I would like to thank all the amazing women in the front office in the Computer Science Department who calm me down when I express a complete lack of knowledge about paperwork, protocol, and procedures. I would like to thank my music library for the writing trances that helped complete each chapter. The group Horse Feathers has been specifically amazing. I would like to thank my university library for access to the many books and articles that influences how I think. The also sometimes purchased books that were relevant to my dissertation. I'd like to thank all the

people who provided feedback when I presented posters and talked about my research at conferences. I've also received numerous scholarships, which have allowed me to travel to said conferences. Thanks for supporting a poor graduate student.

Being a woman in computer science has, in part, made me the woman I am. I'd like to thank the Anita Borg Institute and all the women who have been, and will continue to be, in the Virginia Tech Association for Women in Computing for the continual support. To complement that last comment, last, thanks to all the men in computer science who gave me explicit and implicit warnings that, as a woman, I couldn't cut it. You enrage my inner feminist (read: "bitch"). Thanks for making me push myself harder.

The path to becoming a doctor is littered with distractions. I'd like to thank those distractions for making me the person I am.

## Table of Contents

<b>1</b>	<b>INTRODUCTION.....</b>	<b>1</b>
1.1	NEED .....	1
1.2	RESEARCH QUESTIONS .....	3
1.3	RESEARCH LOCATIONS .....	4
1.4	APPROACH .....	5
1.5	ASSUMPTIONS .....	7
1.6	BENEFITS.....	7
1.7	ALTERNATIVE CHOICES OF STUDY.....	8
1.8	BACKGROUND.....	8
1.9	OUTLINE.....	8
<b>2</b>	<b>RELATED WORK .....</b>	<b>10</b>
2.1	USABLE SECURITY .....	10
2.1.1	<i>History of Usable Security .....</i>	<i>11</i>
2.1.2	<i>The Social Side of Security.....</i>	<i>13</i>
2.2	PRIVACY.....	14
2.2.1	<i>Models of Privacy.....</i>	<i>15</i>
2.2.2	<i>Designing for Privacy .....</i>	<i>17</i>
2.2.3	<i>Software Designed for Privacy.....</i>	<i>18</i>
2.2.4	<i>Evaluations of User Privacy.....</i>	<i>19</i>
2.3	RELEVANT STUDIES OF THE MANAGEMENT OF SENSITIVE INFORMATION .....	19
2.3.1	<i>Articulation Work.....</i>	<i>19</i>
2.3.2	<i>Abstract Places &amp; Spaces.....</i>	<i>21</i>
2.3.3	<i>Physicians' Offices.....</i>	<i>21</i>
2.3.4	<i>Childcare Centers.....</i>	<i>23</i>
2.4	BREAKDOWNS .....	24
2.4.1	<i>Research Utilizing Breakdowns as an Analytical Framework.....</i>	<i>25</i>
2.5	SUMMARY .....	26
<b>3</b>	<b>METHOD.....</b>	<b>27</b>
3.1	PARTICIPANTS & LOCATIONS .....	27
3.1.1	<i>Rural &amp; Urban Virginia .....</i>	<i>28</i>
3.1.2	<i>Description of Childcare Centers.....</i>	<i>30</i>
3.1.3	<i>Description of Physicians' Offices.....</i>	<i>36</i>
3.1.4	<i>Multi-site Fieldwork.....</i>	<i>39</i>
3.1.5	<i>Participant Demographics .....</i>	<i>39</i>
3.2	DATA COLLECTION IN CHILDCARE CENTERS AND PHYSICIANS' OFFICES.....	43
3.2.1	<i>Sampling Method.....</i>	<i>44</i>
3.2.2	<i>Protocols for Conducting Interviews &amp; Observations .....</i>	<i>44</i>
3.2.3	<i>Participant Recruitment for Interviews &amp; Observations.....</i>	<i>46</i>
3.2.4	<i>Training &amp; Preparing for Interviews &amp; Observations.....</i>	<i>47</i>
3.2.5	<i>Data Management .....</i>	<i>49</i>
3.2.6	<i>Dates &amp; Times of Observations.....</i>	<i>50</i>
3.2.7	<i>Transcribing Data .....</i>	<i>53</i>
3.3	DATA ANALYSIS .....	53
3.3.1	<i>Combining Data Across Study and Location .....</i>	<i>54</i>
3.3.2	<i>Activity Theory as a response to Research Question 1 .....</i>	<i>54</i>
3.3.3	<i>Phenomenology as a Response to Research Question 2 .....</i>	<i>58</i>
3.3.4	<i>Near-Future Scenarios as a Response to Research Question 3.....</i>	<i>64</i>
3.4	SUMMARY .....	65

<b>4</b>	<b>PRIVACY &amp; SECURITY RELATED BREAKDOWNS.....</b>	<b>66</b>
4.1	POLICY VIOLATIONS .....	66
4.1.1	<i>HIPAA Violations .....</i>	67
4.1.2	<i>Doctors Exchanging Client Information .....</i>	67
4.1.3	<i>Knowing Patients Personally .....</i>	68
4.1.4	<i>Staff Accessing Client Information that they Should Not Access .....</i>	68
4.1.5	<i>Client’s Family, Friend, and Neighbors Discussing Client Information .....</i>	70
4.1.6	<i>Sharing Login .....</i>	71
4.1.7	<i>Disregarding Privacy Policy.....</i>	72
4.1.8	<i>Lack of Password Use .....</i>	75
4.2	BELIEFS ABOUT SECURITY .....	76
4.2.1	<i>Incorrect Beliefs About Technology.....</i>	76
4.2.2	<i>Menacing Outsider .....</i>	77
4.2.3	<i>Parents Lacking Confidence in Childcare Centers Keeping Information Safe.....</i>	77
4.2.4	<i>Parents Not Knowing Who Can Access Their Child’s File.....</i>	79
4.3	HUMAN-TECHNOLOGY MISMATCH .....	79
4.3.1	<i>Difficulty Locating Client File .....</i>	80
4.3.2	<i>Inability to use Electronic System Results in Information Duplication .....</i>	80
4.4	INADEQUATE REPRESENTATION IN AVAILABLE INFORMATION SYSTEM.....	81
4.4.1	<i>Client Providing Perceived Unnecessary Information.....</i>	81
4.4.2	<i>Fields Not Providing Enough Patient Information .....</i>	82
4.4.3	<i>Not Knowing Who Accessed or Modified Client Information .....</i>	82
4.5	INFORMATION ACQUISITION .....	83
4.5.1	<i>Difficulties Gathering Information from Parents/Staying Up to Date on New Information .....</i>	83
4.5.2	<i>Patients Not Recognizing Updated Information .....</i>	85
4.5.3	<i>When Staff Does Not Document “Adequately” .....</i>	85
4.6	INFORMATION SYSTEM PROBLEMS.....	85
4.6.1	<i>Client Information is Permanent.....</i>	85
4.6.2	<i>Electronic Record Systems Crashing &amp; Loosing Client Information (and Fears) ...</i>	86
4.7	INFORMATION WITHHELD OR HIDDEN .....	88
4.7.1	<i>Childcare Center Obscuring Information .....</i>	88
4.7.2	<i>Office Staff Hiding Information.....</i>	88
4.7.3	<i>Patient Confusion Over Procedure .....</i>	88
4.8	LOCAL NEGOTIATION OF CONTENT .....	89
4.8.1	<i>Auditing and Preparing for Incorrect Patient Information.....</i>	89
4.8.2	<i>Filling in Missing Content.....</i>	90
4.8.3	<i>Hesitation About Writing or Storing Client Information (Suspected Abuse) .....</i>	91
4.8.4	<i>Not Providing “Necessary” Information .....</i>	93
4.8.5	<i>Situations When there is a Need to Disclose More Information than “Normal” ....</i>	94
4.9	LOCAL NEGOTIATION OF POLICY .....	94
4.9.1	<i>Missing Child .....</i>	94
4.9.2	<i>Inappropriate Disclosure of Incorrect Patient Information.....</i>	95
4.9.3	<i>Licensing Problems .....</i>	95
4.9.4	<i>Pharmaceutical Representatives &amp; Insurance Companies Seeking Patient Information.....</i>	99
4.9.5	<i>Receptionist Functioning as Nurse.....</i>	99
4.9.6	<i>Staff Catching Incorrect Medical Procedure .....</i>	100
4.10	ACCESS POLICY .....	100
4.10.1	<i>Parental Over Restriction of Access.....</i>	100
4.10.2	<i>Restricting Client Access to Files.....</i>	101

4.11	SENSITIVE INFORMATION PUBLICALLY ACCESSIBLE .....	102
4.11.1	<i>Open Access to Client Information</i> .....	102
4.11.2	<i>Patient Information Left in the Open</i> .....	103
4.11.3	<i>Children’s Pictures on Facebook</i> .....	104
4.11.4	<i>Client Files Dispersed in Environment</i> .....	104
4.11.5	<i>Disclosing Patient Information</i> .....	107
4.11.6	<i>File Being Kept Outside of Office</i> .....	108
4.12	SYNCHRONIZING INFORMATION WITH REALITY .....	108
4.12.1	<i>Difficulties with Client Care when Outside of the Center</i> .....	109
4.12.2	<i>Getting Information that is Purposefully Not in the File</i> .....	109
4.12.3	<i>Incorrect or Unresolved Information in the Patient File</i> .....	110
4.12.4	<i>Looking Up Patients on Sex Offender Website</i> .....	110
4.12.5	<i>Lost Paper Patient File</i> .....	110
4.12.6	<i>Missing Client Information</i> .....	111
4.12.7	<i>Missing Documentation to go into a Client File</i> .....	111
4.12.8	<i>Missing Electronic File</i> .....	111
4.12.9	<i>Permanently Missing (or Dead) Client</i> .....	112
4.12.10	<i>Recalling Codes</i> .....	112
4.13	SUMMARY .....	113
<b>5</b>	<b>THE PHENOMENON OF SECURITY AND PRIVACY IN MANAGING SENSITIVE CLIENT INFORMATION .....</b>	<b>115</b>
5.1	PRIVACY & SECURITY EMBODIMENT .....	115
5.1.1	<i>Where Privacy and Security are Not Located</i> .....	117
5.1.2	<i>Where Privacy and Security are Located</i> .....	121
5.1.3	<i>Summary</i> .....	125
5.2	COMMUNITIES OF SECURITY .....	126
5.2.1	<i>The Value of Roles in Relation to Communities of Security</i> .....	127
5.2.2	<i>The Value of Relationships in Security and Privacy</i> .....	129
5.2.3	<i>Summary</i> .....	133
5.3	ZONES OF AMBIGUITY .....	134
5.3.1	<i>Ambiguities</i> .....	134
5.3.2	<i>Client Agency &amp; Ambiguity</i> .....	141
5.4	SUMMARY .....	142
<b>6</b>	<b>PRIVACY &amp; SECURITY SCENARIOS.....</b>	<b>144</b>
6.1	ASSUMPTIONS EMBEDDED WITHIN THE SCENARIOS.....	144
6.2	SCENARIOS REPRESENTING SPECTRUM ENDS .....	145
6.2.1	<i>Access v. Inaccess</i> .....	145
6.2.2	<i>Anonymity v. Visibility</i> .....	147
6.2.3	<i>Permanence v. Decay</i> .....	150
6.2.4	<i>Centralization v. Decentralization</i> .....	152
6.2.5	<i>Layered v. Flat</i> .....	154
6.2.6	<i>Contextual Awareness v. Lack of Contextual Awareness</i> .....	156
6.2.7	<i>Center-managed Privacy v. Client-managed Privacy</i> .....	158
6.2.8	<i>Technical v. Social Enforcement</i> .....	161
6.3	DISCUSSION.....	163
6.3.1	<i>Seamless and Seamful</i> .....	163
6.3.2	<i>The Surveillance of Security</i> .....	164
6.3.3	<i>“Do Nothing” Scenario</i> .....	164
6.4	SUMMARY .....	165

<b>7</b>	<b>CONCLUSION.....</b>	<b>167</b>
7.1	PAPER VERSUS ELECTRONIC CLIENT FILES .....	169
7.2	FUTURE WORK.....	170
7.3	RESEARCHER REFLECTIONS.....	171
<b>8</b>	<b>REFERENCES.....</b>	<b>174</b>
<b>9</b>	<b>APPENDIX A, OBSERVED BREAKDOWNS.....</b>	<b>186</b>
9.1	GETTING INFORMATION THAT IS PURPOSEFULLY NOT IN THE FILE (STUDY 2).....	186
9.2	INCORRECT OR UNRESOLVED INFORMATION IN THE PATIENT FILE (STUDY 2).....	188
9.3	PROACTIVELY SHARING KNOWLEDGE NOT IN CLIENT FILE (STUDY 2).....	191
9.4	RECALLING CODES (STUDY 2).....	192
9.5	PERMANENTLY MISSING (OR DEAD) CLIENT (STUDY 2).....	194
9.6	MISSING DOCUMENTATION TO GO INTO A CLIENT FILE (STUDY 2).....	195
9.7	UNAWARE OF CLIENT LOAD (STUDY 2).....	198
9.8	MISSING ELECTRONIC FILE (STUDY 2).....	200
9.9	CLIENT PROVIDING PERCEIVED UNNECESSARY INFORMATION (STUDY 1).....	203
9.10	CLIENT PROVIDING PERCEIVED UNNECESSARY INFORMATION (STUDY 2).....	204
9.11	DISCONNECT BETWEEN DISPERSED PATIENT INFORMATION (STUDY 2).....	206
9.12	DISCLOSING PATIENT INFORMATION (STUDY 2).....	209
9.13	AUDITING AND PREPARING FOR OFFICE’S INCORRECT PATIENT INFORMATION (STUDY 1).....	212
9.14	AUDITING AND PREPARING FOR OFFICE’S INCORRECT PATIENT INFORMATION (STUDY 2).....	213
9.15	KNOWING A PATIENT’S PRIVATE CIRCUMSTANCES (STUDY 2).....	214
9.16	LACK OF PASSWORD USE (STUDY 1).....	217
9.17	LACK OF PASSWORD USE (STUDY 2).....	217
9.18	DIFFICULTY LOCATING CLIENT FILE (STUDY 1).....	219
9.19	DIFFICULTY LOCATING CLIENT FILE (STUDY 2).....	220
9.20	INAPPROPRIATE DISCLOSURE OF INCORRECT PATIENT INFORMATION (STUDY 2).....	222
9.21	OFFICE STAFF HIDING INFORMATION (STUDY 2).....	225
9.22	PATIENT CONFUSION OVER PROCEDURE (STUDY 2).....	226
9.23	MISSING CLIENT INFORMATION (STUDY 1).....	227
9.24	MISSING CLIENT INFORMATION (STUDY 2).....	228
9.25	HIPAA VIOLATIONS (STUDY 2).....	229
9.26	TASK INTERRUPTION DISRUPTS MANAGING CLIENT INFORMATION (STUDY 1).....	232
9.27	TASK INTERRUPTION DISRUPTS MANAGING CLIENT INFORMATION (STUDY 2).....	232
9.28	KNOWING PATIENTS PERSONALLY (STUDY 2).....	234
9.29	DIFFICULTIES BETWEEN EXTERNAL OFFICES SHARING PATIENT INFORMATION (STUDY 2).....	235
9.30	OFFICE RELATIONSHIPS AFFECTING CLIENT CARE (STUDY 1).....	236
9.31	OFFICE RELATIONSHIPS AFFECTING CLIENT CARE (STUDY 2).....	237
9.32	STAFF CATCHING INCORRECT MEDICAL PROCEDURE (STUDY 2).....	240
9.33	LOOKING UP PATIENTS ON SEX OFFENDER WEBSITE (STUDY 2).....	241
9.34	PHARMACEUTICAL REPRESENTATIVES & INSURANCE COMPANIES SEEKING PATIENT INFORMATION (STUDY 1).....	242
9.35	PHARMACEUTICAL REPRESENTATIVES & INSURANCE COMPANIES SEEKING PATIENT INFORMATION (STUDY 2).....	243
9.36	DISREGARDING PRIVACY POLICY (STUDY 1).....	244
9.37	DISREGARDING PRIVACY POLICY (STUDY 2).....	245
9.38	DIFFICULTIES WITH CLIENT CARE WHEN OUTSIDE OF OFFICE/CENTER (STUDY 1).....	246
9.39	DIFFICULTIES WITH CLIENT CARE WHEN OUTSIDE OF OFFICE/CENTER (STUDY 2).....	247

9.40	PATIENT INFORMATION LEFT IN THE OPEN (STUDY 2) .....	249
9.41	INABILITY TO USE ELECTRONIC SYSTEM RESULTS IN INFORMATION DUPLICATION (STUDY 2) .....	250
9.42	RESTRICTING CLIENT ACCESS TO FILES (STUDY 1) .....	251
9.43	RESTRICTING CLIENT ACCESS TO FILES (STUDY 2) .....	256
9.44	NOT KNOWING WHO ACCESSED/MODIFIED CLIENT INFORMATION (STUDY 1) .....	257
9.45	FILE BEING KEPT OUTSIDE OF THE OFFICE (STUDY 1).....	259
9.46	OPEN ACCESS TO CLIENT INFORMATION (STUDY 1).....	262
9.47	OPEN ACCESS TO CLIENT INFORMATION (STUDY 2).....	266
9.48	LACK OF KNOWLEDGE OF WHAT TO DO IF SOMETHING GOES “WRONG” (STUDY 1) .....	267
9.49	ELECTRONIC RECORD SYSTEMS CRASHING & LOOSING CLIENT INFORMATION (AND FEARS) (STUDY 1).....	267
9.50	ELECTRONIC RECORD SYSTEMS CRASHING & LOOSING CLIENT INFORMATION (AND FEARS) (STUDY 2).....	269
9.51	NOT PROVIDING “NECESSARY” INFORMATION (SSN) (STUDY 1).....	271
9.52	HESITATION ABOUT WRITING/STORING CLIENT INFORMATION (SUSPECTED ABUSE) (STUDY 1) .....	272
9.53	LOST PAPER PATIENT FILE (STUDY 1).....	279
9.54	“INAPPROPRIATE” STAFF ACCESS OF CLIENT INFORMATION (STUDY 1).....	279
9.55	CLIENT’S FAMILY/FRIEND/NEIGHBORS DISCUSSING CLIENT INFORMATION (STUDY 1).....	280
9.56	CLIENT’S FAMILY/FRIEND/NEIGHBORS DISCUSSING CLIENT INFORMATION (STUDY 2).....	283
9.57	DOCTORS EXCHANGING CLIENT INFORMATION (STUDY 1).....	283
9.58	RECEPTIONIST FUNCTIONING AS NURSE (STUDY 2).....	285
9.59	FIELDS NOT PROVIDING ENOUGH PATIENT INFORMATION (STUDY 2).....	285
9.60	PATIENTS NOT RECOGNIZING UPDATED INFORMATION (STUDY 2).....	287
9.61	SHARING LOGIN (STUDY 1) .....	287
9.62	SHARING LOGIN(STUDY 2) .....	288
9.63	(TEMPORARILY) MISSING CHILD (STUDY 1) .....	290
9.64	(TEMPORARILY) MISSING CHILD (STUDY 2) .....	296
9.65	DIFFICULTIES GATHERING INFORMATION FROM PARENTS/STAYING UP TO DATE ON NEW INFORMATION (STUDY 1).....	297
9.66	DIFFICULTIES GATHERING INFORMATION FROM PARENTS/STAYING UP TO DATE ON NEW INFORMATION (STUDY 2).....	299
9.67	CLIENT FILES DISPERSED IN ENVIRONMENT (STUDY 1) .....	301
9.68	PARENTAL OVER RESTRICTION OF ACCESS (STUDY 1).....	305
9.69	SECURING CHILDREN (STUDY 1) .....	307
9.70	STAFF ACCESSING CLIENT INFORMATION THAT THEY SHOULD NOT ACCESS (STUDY 1).....	310
9.71	SENSITIVE INFORMATION DISPLAYED IN ENVIRONMENT (STUDY 1).....	312
9.72	LICENSING ISSUES (STUDY 1).....	313
9.73	INCORRECT BELIEFS ABOUT TECHNOLOGY (STUDY 2).....	319
9.74	INCORRECT BELIEFS ABOUT TECHNOLOGY (STUDY 1).....	320
9.75	DIFFICULTIES COMMUNICATING WITH FOREIGN PARENTS (STUDY 2) .....	322
9.76	WHEN STAFF DOES NOT DOCUMENT “ADEQUATELY” (STUDY 2) .....	323
9.77	CLIENT INFORMATION IS PERMANENT (STUDY 1).....	324
9.78	SITUATIONS WHERE THERE IS A NEED TO DISCLOSE MORE INFORMATION THAN “NORMAL” (STUDY 1).....	330
9.79	FILLING IN MISSING INFORMATION (STUDY 1).....	331

9.80	MENACING OUTSIDER (STUDY 2) .....	332
9.81	CHILDCARE OBSCURING INFORMATION (STUDY 1) .....	333
9.82	PARENTS NOT KNOWING WHO CAN ACCESS THEIR CHILD’S FILE (STUDY 1).....	335
9.83	PARENTS LACKING CONFIDENCE IN CHILDCARE KEEPING INFORMATION SAFE (STUDY1) .....	339
9.84	CHILDREN’S PICTURES ON FACEBOOK (STUDY 1).....	342
<b>10</b>	<b>APPENDIX B, LIST OF INFORMED CONSENTS .....</b>	<b>344</b>
<b>11</b>	<b>APPENDIX C, LIST OF INSTRUMENTS .....</b>	<b>356</b>

## List of Figures

Figure 1. Three scenarios depicting levels of overlap between social and technical security mechanisms in the protection of sensitive personal information. ....	3
Figure 2. Map of average household income for the New River Valley, Virginia where the income is between less than \$18,000 and \$27,000. ....	29
Figure 3. Pictures from different four childcare center directors' offices. ....	31
Figure 4. Sample floor plan for a childcare center. ....	34
Figure 5. Front desk of a childcare center. There is a monitor and picture frame in the corner. Desk and 1-way mirror on the other corner behind (Branham et al. 2009)..	35
Figure 6. Displays of HIPPA regulation in physician’s office. ....	36
Figure 7. A physician’s office’s files located on the surrounding walls of the director's office. ....	38
Figure 8. A visual representation of the different participant types. ....	40
Figure 9. Sample of how memos were used to bracket interpretations and notes. ....	49
Figure 10. The form of an activity at the individual level, sometimes called Mediation Model (Mwanza 2001). ....	55
Figure 11. An Activity from the community and individual perspective, sometimes called the Activity Triangle Model (Engeström 1987; Mwanza 2001). ....	56
Figure 12. The phases of analysis when conducting phenomenological qualitative inquiry. ....	60
Figure 13. NAYCE required form that asks parents to select who can access their child's information. ....	69
Figure 14. Sample patient privacy polices displayed in the waiting rooms of physicians' offices. ....	73
Figure 15. Sample patient privacy policy displayed in the waiting room of a physician's office explaining how records are retained and destroyed. ....	74
Figure 16. Example "Read Me" sign used in childcare centers to encourage parents to read the bulletin. ....	84
Figure 17. Sign-in and Sign-out sheet from Child-P03. ....	91
Figure 18. The one page condensed version of interpreted licensing requirements. ....	98
Figure 19. Med-P01's client files open for anyone to access. ....	103
Figure 20. Six pictures depicting the places where information about children is stored. ....	106
Figure 21. Med-P15’s electronic file system called “e-MD.” ....	113
Figure 22. Med-P01's electronic file system. ....	113
Figure 23. A hypothetical user interface similar to Facebook for managing client information. ....	159
Figure 24. Sample of an electronic seam. ....	164

## List of Tables

Table 1. A list of research questions, methods used to respond to research questions, why that method is appropriate, and what section in the dissertation that question is answered. ....	4
Table 2. Research Problems, Goals, and Approaches .....	6
Table 3. Research Questions.....	27
Table 4. Characteristics of the participating childcare centers. ....	41
Table 5. Demographic information for the parents who participated in our study .....	42
Table 6. Characteristics of the participating physicians' offices, when the first contact or interview(s) took place, and the people who were interviewed. ....	42
Table 7. Dates and times of observations of childcare centers in Study 1.....	50
Table 8. The dates and times of Study 2 observations with childcare center and physician's office directors. ....	51
Table 9. The times of observations at childcare centers visually depicted to demonstrate that all times of the day were observed. ....	52
Table 10. The times of observations at physicians' offices visually depicted to demonstrate that all times of the day were observed. ....	53
Table 11. Breakdown themes used to describe the breakdowns relating to security and privacy. ....	63

# 1 Introduction

Traditionally, electronic and physical security has been concerned with creating rules, locks, and passwords. However, security systems that neglect people as a significant part of the equation “are seldom secure in practice” (Bellotti et al. 1993). Practice is what happens in the moment; it is the activity; it is what is actually done. It is often in the human-centered moment, and not in the computer-centered planning stages, when security policies or mechanisms break down and the safety of sensitive information is compromised (Adams et al. 1999; Dourish et al. 2004; Adams et al. 2005a). When a breakdown occurs in a social system (as opposed to a computational one), workers do not stop what they are doing. Instead, they create special cases or methods that allow them to continue by adapting formal work policies, e.g., when users write passwords on post-it notes, or shout them across the room (Adams et al. 1999; Dourish et al. 2004; Adams et al. 2005a). As a result, there exists a need to study and to understand the holistic practice and experience of security management in socio-technical systems (Dourish et al. 2006). In this dissertation I present the study of childcare centers and physicians' offices as representative examples of the collaborative management of sensitive information in professional environments.

The primary work of childcare centers and physicians' offices inevitably becomes entwined with managing information that is integral to both their everyday operations and long-term licensure. Most information is routine, but some is sensitive. For these reasons licensed childcare providers and physicians' offices in the United States provide a rich environments for understanding complex, sensitive, and collaborative information management problems as they pertain to privacy and security (Baker et al. 2011a; Baker et al. 2011b). This study seeks to understand how work practices are affected by the breakdowns that occur within explicit and implicit policies in settings that work with sensitive personal information. The purpose of this work is to contextualize the role of practice in security literature through the use of qualitative data and user-centered analysis. This will be accomplished through the collection of interviews and observations with childcare centers and physicians' offices in the New River Valley of Southwest Virginia. The results from this study will provide insight into producing electronic and physical security mechanisms that support collaborative work practice.

## 1.1 Need

Prior work has examined childcare centers and physicians' offices, focusing on how systems can support individuals engaging in security and privacy practices. For example, prior research on privacy has examined how plans, work, and documentation are mediated by artifacts (Kientz et al. 2009a), how models and frameworks can be used to design for privacy (Whitten et al. 1999), and the effects of deploying technology probes aimed at exploring security and privacy (Bylund et al. 2008). However, the study of how current work *practices* of communities are maintained, and how they secure sensitive information is an area with a small but growing interest within the larger area of security research (Adams et al. 1999; Adams et al. 2005a; Flechais et al. 2005; Dourish et al. 2006).

For the purpose of this research, I define privacy as a situated and negotiated construct, and based the definition off of the work of privacy from the domain of Human-Computer Interaction (Harrison et al. 1996; Palen et al. 2003; Dourish et al. 2006). In particular, the work of Palen and Dourish defines privacy, and security as the protection of privacy, as a dialectic and boundary regulation process. It is dialectic because it is individually based on the actor's experiences along with the experiences of interacting with others who also have unique perspectives. It is a boundary regulation process because privacy is being continuously negotiated based on the contextual situation related to what should and should not be disclosed (Palen et al. 2003). For the purpose of this definition, sensitive information is defined as any information that is private, yet must be managed by a subset of the population for the care of the client. Security and privacy systems are ones that attempt to account for how to protect sensitive data by protecting unwanted users. Examples include protecting online patient information (Gammon 2010), protecting online social identities (Fogel et al. 2009), and protecting online court records (Sudbeck 2006). It is with these definitions in mind that I consider security practices, especially in regard to how they are embodied in the management of sensitive personal information.

Security and privacy are increasingly being automated with technology through the increasing adoption of centralized content and information sources (Pinner 1998; Vaidyanathan et al. 2009), the sharing of location-based information (Harper et al. 1992; Gellersen et al. 2002; Bardram 2009a), and the management of online identities (Friedewald et al. 2007). The use of programmable policies and role-based ontologies has facilitated technology to create the appearance that the information and data is secure, e.g., (Thuraisingham 2005; Huang et al. 2006; Chowdhury et al. 2007). This increase in the use of automated security carries with it an implied assumption that these technical measures are more effective than the previously used social ones. The term "social" refers to the communication, sharing, and interrelationships that are co-constructed through interaction in work systems. My argument, however, is that the increased use of technology may not increase the security of sensitive personal information unless social measures are accounted for. For example Flechais et al. argue that social systems are inherently flexible and can detect nuances, whereas technical systems are reliable and lack bias (2005). Similarly, the work of Palen & Dourish, Harrison & Dourish, and Dourish & Anderson all argue that privacy is an inherently social construct that defies automation in a changing socio-technical landscape (Harrison et al. 1996; Palen et al. 2003; Dourish et al. 2006).

To demonstrate this argument, I provide in Figure 1 three different levels of overlap between social and technical mechanisms. For the purpose of this dissertation, I adopt the definition of socio-technical systems from Flechais et al. as one comprised of people and technology that interact in the shared task of safe praxis (Flechais et al. 2005). In the diagram, the square box that the circles enclose represents the entire space of sensitive personal information that is to be managed in a workplace. The diagram on the left depicts the current state of use in regards to technical and social mechanisms: there is some overlap between measures that are both socially and technically accounted for, but there is much that is handled by only social or technical mechanisms. The second figure shows the increasing use of technology, also supporting more of the realm of how

sensitive personal information is being managed. In this depiction, there is still overlap between the social and technical, along with some social mechanisms (e.g., whispering) that are used. What I am proposing is that design could be used to optimize and use both social and technical mechanisms to create secure practice. This optimization is depicted in the right-hand diagram. I argue that by combining and optimizing the parts of the system that should be supported with technical mechanisms and the parts of the system that should be supported by social mechanisms, that a better system can be designed. Specifically, this system would be one that would not be circumvented by the users, e.g., (Whitten et al. 1999; Brustoloni et al. 2007).

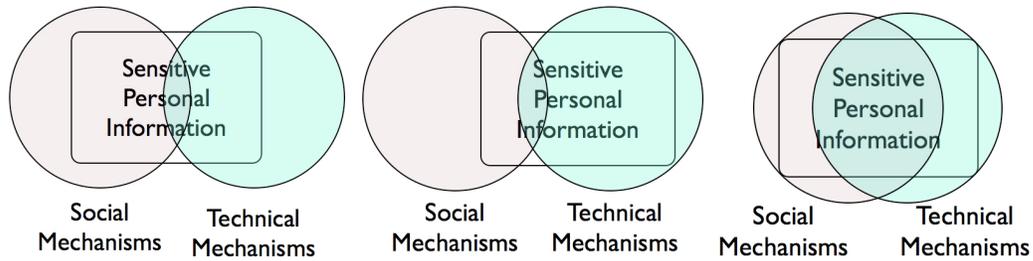


Figure 1. Three scenarios depicting levels of overlap between social and technical security mechanisms in the protection of sensitive personal information.

The larger encompassing goal of this work is to determine the optimal use of technical, social, and socio-technical mechanisms to support the best management of sensitive personal information. The concept has been called “joint optimization” in the socio-technical system theory literature, and means that there is an equality between the technical performance and the quality of the lives of the people (Trist et al. 1997; Baskerville et al. 2000; Kleiner 2004). Socio-technical systems theory recognizes that there are social and technical aspects of a work system that produce social and psychological outcomes along with physical products. The ambition of the socio-technical designer is to optimize both the social and technical mechanisms for the best design and user interaction. My central argument is two points: (1) that there is a need for a larger overlap between the social and technical will result in dynamic, flexible, and reliable security mechanisms, and (2) to understand how to design this system there is a need to study the socio-technical systems.

## 1.2 Research Questions

Responding to the need for research in this area, my research question is, “How do socio-technical systems that use sensitive personal information manage breakdowns surrounding the implicit and explicit rules of process?”

I have further broken this down into three sub-questions:

- What breakdowns occur when the explicit and implicit rules are not followed?
- How are breakdowns responded to, negotiated, and managed in socio-technical systems where sensitive personal information exists?
- What are the implicit and explicit rules surrounding how physicians’ offices and childcare centers handle sensitive personal information?

Table 1. A list of research questions, methods used to respond to research questions, why that method is appropriate, and what section in the dissertation that question is answered.

<b>Research Question</b>	<b>Method</b>	<b>Why</b>	<b>Dissertation Section</b>
What breakdowns happen when the explicit and implicit rules are not followed?	Used Activity Theory's definition of breakdown to identify conflicts in the activity system related to security & privacy.	The subject-object analysis provided by Activity Theory provides a framework for eliciting breakdowns in socio-technical systems.	Chapter 4, Appendix A
How are breakdowns accounted for, negotiated, and managed in socio-technical systems where sensitive personal information exists?	Used Phenomenological analysis of breakdowns to synthesize experience of security and privacy.	Phenomenology again uses the subject-object relationship to examine constructs like security and privacy to understand the outcome and experiences of the participants.	Chapters 4 & 5
What are the implicit and explicit rules surrounding how physicians' offices and childcare centers handle sensitive personal information?	Used Scenarios to enumerate and depict specific practices in order to demonstrate spectrums of rules surrounding security and privacy.	Scenarios provide a rich mechanism for detailing constructs into representative practice.	Chapter 6

### ***1.3 Research Locations***

The work presented in this dissertation examines security-in-practice by engaging in communities that are rich in sensitive information that is managed through significant amounts of collaborative documentation, access, and retrieval. The two domains I have explored are the childcare center domain and the physician's office domain. The study of these locations is becoming ever more necessary as we strive to design secure and usable systems for childcare centers and physicians' offices, which are increasingly adopting digital documentation systems (Berner et al. 2005; Jha et al. 2006).

In these domains the adversarial actions are unintentional, unwelcome, and intrusive access and modification of sensitive personal information. Examples include physician's

office and childcare center personnel, external people, and insurance companies accessing patient or child information that should be private. A second example includes “work-around” practices of the personnel themselves that result in unknown and unsecure information disclosures.

Electronic systems are being increasingly adopted in the collaborative management of information (Hart et al. 1997; Premkumar et al. 1999; Berner et al. 2005). However, little research has explored how the adoption of these systems will affect the larger socio-technical system. We therefore present the childcare centers as a rich location to study. They represent interesting locations because of the need to balance two tasks: (1) the need for privacy in regards to the management of a child’s file, and (2) the collaborative management of care and information between staff, external people, and parents. Childcare centers are a significant setting in the United States because of its prevalence and importance in people’s lives. According to the US Census Bureau, of the working parents in 2008 approximately 66% have both a mother and a father in the labor force (2009). With both parents working, there is a need for childcare solutions. Childcare centers have programs for infants and pre-schoolers, and also provide after-school care for elementary age children. According to the U.S. Department of Education, National Center for Education Statistics, thirty-six percent of all children under six who are not yet in kindergarten participate in childcare centers (2005). Little research has explored the two sides of childcare: the day-to-day practices of educating, nourishing, and keeping a child safe, and the documentary regulatory service that is licensed and governed by state codes of conduct. For more information please see Virginia’s Department of Social Services documentation on childcares: (2010a).

Additionally physicians’ offices are also valuable locations of study because there is a plethora of sensitive patient information that exists in various stages and forms of documentation. Physicians’ offices are valuable locations of study given the collaborative nature of the work and the increasing adoption of electronic medical records (Berner et al. 2005). However, it is expected that patients will gain a heightened awareness and concern for the security of their medical records as patient agency increases (Merrill 2011). There has been an “endemic failure” to adapt to advancing best practices and technology that has created “antiquated data security, governance, policy plaguing the healthcare industry.” This has been similarly argued by healthcare security experts (Merrill 2010; Merrill 2011). Digital security in the healthcare industry has not adapted to meet current challenges. However, despite the obvious need for increased information security in physicians’ offices, little work is being done in the area.

#### ***1.4 Approach***

This study was conducted in two parts: Study 1 and Study 2. Study 1 involved the collection of 21 interviews with parents, 13 interviews with physician’s office directors, 12 interviews with childcare center directors, and 27 hours of observation of childcare centers. This data was presented in my proposal defense. Post-proposal an additional 96 hours of observations of childcare centers and physicians’ offices along with two additional interviews of physician’s office directors was conducted. Together this data represents the body of data considered in this dissertation.

To analyze the data a phenomenological approach was used to study the essence of security and privacy in the offices that manage sensitive client information. This involved the transcription of all interviews, observation notes, forms, and pictures.

To analyze security and privacy, this dissertation focuses on breakdowns, as defined by Activity Theory, as a theoretical lens. Using this lens I have focused the body of data down to 281 breakdowns where the socio-technical system did not support the users in their task of managing privacy and security. These breakdowns were then combined by similar breakdowns (e.g., offices that shared passwords). Breakdowns were then thematically organized, and are presented in Chapter 4. The discussion and analysis of these themes and breakdowns is presented in Chapter 5 as the essence of security and privacy in this socio-technical system.

Table 2. Research Problems, Goals, and Approaches

<b>Problem</b>	<b>Goal</b>	<b>Approach</b>
Prior work has highlighted that security is put into practice through explicit and implicit policies. However, little work exists that examines the policies involved in the collaborative management of sensitive information.	To examine the current work practices to understand the policies are made explicit and what policies are left implicit for security.	To interview relevant stakeholders in the management of personal sensitive information.
Given an understanding of explicit and implicit policies, there has been little work to understand how these practices are then actualized in the collaborative management of sensitive personal information.	To compare what has been traditionally thought of as security to how communities manage security in practice.	To observe the work of managing personal sensitive information.
Breakdowns occur in all systems of interaction. However, there is little understanding of how breakdowns affect security practices and policy adaptations.	To detail all observed and discussed breakdowns as they relate to security and privacy.	With the use of Activity Theory, to analyze interviews and observations for response to breakdowns in security.

## ***1.5 Assumptions***

This work represents some key assumptions about the field of electronic record keeping and socio-technical systems. The first is the assumption that electronic record keeping is a growing field; childcare centers and physicians' offices will eventually be paperless environments. This assumption leads to the conclusion that as electronic systems are increasingly adopted they will influence and change the way that people behave in offices. Some of those behavior changes will be security and privacy practices.

The second assumption is that by being an active participant in the work practice, I will observe actual security policies. The Heisenberg Uncertainty Principle states that merely watching a phenomenon will cause it to change. To apply this principle to the work presented in this dissertation, observing the people in the centers will cause their security behaviors to change. I have tried to mitigate this problem by interacting with and observing many different locations to create generality across findings.

A third assumption is that by focusing on breakdowns, I can understand deeply the phenomenon of security and privacy in these settings; that this focus will not overly limit my understanding of the constructs.

The last assumption is that, by studying both childcare centers and physicians' offices, these locations will provide interesting datum to compare and contrast in order to understand the phenomenon.

## ***1.6 Benefits***

This work will benefit the security, the usable security, and the human-computer interaction communities by detailing a deep understanding of how centers manage client information. Resulting from this work will emerge properties that will help the design community to create technology and tools to support secure work practice.

A second benefit from this work will be the conceptualization of security as more than rules. The application of the activity theory framework provides a lens for examining how groups internalize and externalize the constructs of security, trust, and privacy. Activity theory literature on breakdowns will provide additional methods of analysis to the security literature. Additionally, there has been a dearth of research studying how groups manage and coordinate security and put these constructs into practice. This work will add to that body of literature and understanding.

A last benefit of this work will be the use of the outcomes of this work. The two outcomes are a set of categories of breakdowns that occur, and also a set of near-future scenarios depicting consequences of contrasting designs. These two outcomes will provide insight into future work on electronic health records, paperless work systems, and sensor-based privacy research.

## ***1.7 Alternative Choices of Study***

Two choices have been made to make this work valuable. The first is the location of study. It was critical to select areas where privacy was being managed in practice. The settings of childcare centers and physicians' offices were selected because they are similar in their goal of manage and respect sensitive personal information. Childcare centers were selected because they are settings where manipulation and access are more-easily granted. Privacy concerns may not be as highly prevalent because the information is about children, and not life-critical. Physicians' offices were selected because of their daily use of information and because there is a life-critical aspect of making sure that the information is correct. By studying both areas my desire is to better understand the broader area of managing sensitive personal information. File management systems that were not studied but considered were employee files, criminal files, student files, and client files.

The second choice of study involves the length and number of settings to study. This was constrained by local conditions and the willingness of the participants. First, the number of childcare centers and physicians' offices in the region is small. Second, participants limited the amount of time they donated to the project. This was due to a number of factors: the research was conducted without funding and even token remuneration for participants was unavailable; participants were thus contributing to the study out of their own goodwill. Additionally the research intruded upon work time and to maintain amicable and cooperative relations with them, we chose to minimize the intrusions of observations and interviews. To compensate the number of research locations was maximized. Alternative approaches to the dissertation would have broadened the geographical location of the study in an attempt to find more participants. Additional participants might have allowed for broader experiences and reoccurring observations.

## ***1.8 Background***

This work stems from the Usable Security Team in the Computer Science Department at Virginia comprised of Steve Harrison, Dennis Kafura, Denis Gracanin, and Francis Quek. This team is explores how practices affect security in healthcare and smart homes (e.g., Virginia Tech Smart Home<sup>1</sup>).

My prior work has examined how users assess web information. This resulted in a novel evaluation method for measuring user trust. I additionally worked on a review of literature on trust an eHealth websites. This work on the theory of trust produced a valuable base to examine how trust is managed in collaborative practice.

## ***1.9 Outline***

The remainder of this document presents the findings of my dissertation project. The following chapter presents a review of related work on the topics and locations of usable security, privacy, physicians' offices and childcare centers, and breakdowns. A thorough presentation is next made of the methods used to collect the data for my dissertation in the third chapter. In the fourth chapter the data is presented to convey the diversity and

---

<sup>1</sup> The webpage for the Lumanhaus: <http://www.solar.arch.vt.edu/>

problems related to security and privacy. In the fifth chapter the data is then conceptualized to present the essence of security and privacy by three topics: security and privacy embodiment, communities of security, and zones of ambiguity. Last, as a product of this work, scenarios from divergent ends of a spectrum are presented and analyzed. Presented in the appendix of this document is a complete analysis of all observed and discussed breakdowns, and all research tools.

## 2 Related Work

This work stems from three areas: human-computer interaction, medical informatics, and usable security. First, the area of human-computer interaction has impacted this work through its ideals: that software should support the user in the work that he or she wants to do; the user is never wrong; and, that adding more technology to a problem does not necessarily solve it. With these ideals in mind, I have approached the need to understand the space of collaborative management of sensitive personal information. The area of studying sensitive personal information is impacted by previous work on privacy and how the design of novel systems is impacting it. A review of this literature is included below.

Second, the need for studying this area has arisen because there has been increasing use of electronic record systems, particularly within the medical context. Previous researchers in the area of medical informatics have explored methodologically and philosophically the use of tools and how they affect interactions. This area presents a rich body of literature that has served as the driving need to study this area, and is thus additionally included below.

Last, there is now recognition in computer security research that security is only *useful* if it is *usable*. Among other issues, usable security investigates aligning security systems and practices with work practices. With these aspects of the research space in mind, a review of relevant literature on usable security and privacy, along with an analysis of the research on these topics in the locations of childcare centers and physicians' offices, is included below.

Also included in my review of related work is a review of how breakdowns have been used to study novel research areas, such as the one presented in this dissertation.

### 2.1 Usable Security

There has been a movement within the security sub-domain of computer science that recognizes that security has two parts: computers and humans. Security research traditionally focused on making rules to protect data, assuming the user of the security was "the enemy" (Adams et al. 1999). Users, after all, were the ones who were writing down their passwords on post-it notes taped to monitors and holding open RFID badge doors for the person behind them. This recent research area, called "Usable Security," has pushed back at this anti-user assumption: "What if users are not the enemy? Instead, what if the problem is that security is infringing on work practices?" Usable Security's proposal is that if security is hard to manage, it is not because the users are at fault. It is because the security mechanisms are incongruent with the user's primary task. To understand the user's task involves understanding the user's needs, practices, and values. Additionally, with computing systems becoming increasingly ubiquitous, they will become more involved and integrated into everyday work; computers are no longer solitary machines under the computer desk. This means that security can no longer be something that is a secondary task and isolated from the user. Security management has to integrate into the tasks of everyday work.

### 2.1.1 History of Usable Security

The recognition of the need for information security systems to be usable, is not entirely a recent topic. In 1973, Saltzer and Schroder identified psychological acceptability as one of the key considerations for computer security (Saltzer et al. 1973). They explained that, for information systems to be secure, the interface needs to be designed for “ease of use, so that users routinely and automatically apply protection mechanisms correctly.” Indeed, the call to secure private information can be traced to 1890 in Warren and Brandeis’s call for the “Right to Privacy” (Warren et al. 1890). However, it was not until the last decade that a real emergence of the value of users in the socio-technical system (as thinking and active decision maker) has been reflected in the literature in the papers like “Users are Not the Enemy” stimulating the emergence of the field usable security (Adams et al. 1999; Cranor et al. 2005).

Some position papers and reports were published that projected how the field of security should change. For example, in 2003 the Computer Research Association reported what they saw as the four challenges of technology as it moves into the future regarding security and trust. They argued that the infrastructure of technology should move beyond simply creating security policies to create policies that are adaptive to the environments: “Security is concerned with letting the right people access the right information and services in a trusted environment” (Spafford et al. 2003, p.10). Of the four challenges that the CRA proposed, two challenges directly relate to usable security: (1) new technical tools that have large societal significance, like electronic healthcare records and electronic voting systems, need to be designed so that people not only trust them but so that they are also secure; and (2) technologies of the future need to be built upon policies that users can trust and understand. In both of these challenges, trust implies that the user not only is willing to use the technology, but that the user will incorporate it into their practices. This article is critical because it highlights that the perceived future of security lies in embedding security into technologies that are usable and that policies that should be adaptive to user needs.

Additional cues to how the field was changing were starting to appear in years following the CRA Report. Conferences like SOUPS<sup>2</sup> (Symposium on Usable Privacy and Security) emerged. Additionally conferences like UbiComp<sup>3</sup>, and IFIPTM<sup>4</sup> (International Conference on Trust Management) started to publish papers on the topic of usable security. Whitten and Tygar published a key paper in 1999. In this paper they proposed that users may not be the cause of security problems; the real culprit is that computer interfaces have not adapted to discourage security breaches (1999). A central tenant of their argument was that the traditional definitions of usability were not specific enough to be used for security software: “Since usable security requires user interface design priorities that are not the same as those of general consumer software, it likewise requires usability evaluation methods that are appropriate to testing whether those priorities have been sufficiently achieved” (Whitten et al. 1999, p.14). To deal with the lack of

---

<sup>2</sup> <http://cups.cs.cmu.edu/soups/2010/>

<sup>3</sup> <http://www.ubicomp2010.org/home>

<sup>4</sup> <http://www.ifip-tm2010.org/doku.php>

specificity, they defined security to be useable if: (1) users are aware of security tasks that need to be performed, (2) users can successfully perform security tasks, (3) when users do commit errors, they are not dangerous errors, and (4) the user's comfort level is high enough to persist in using the security software. Given this definition, the researchers tested a security interface with, what was at that time, a high usability standard. They found that one third of their participants were able to complete their tasks up to their relatively low standards of usable security.

Between this work and the emergence of a rich research field, there were representative papers from other fields such as human-computer interaction (Friedman et al. 2000), electronic commerce (Head et al. 2002), and security (Hassanein et al. 2004). However, in 2005 Garfinkel and Miller published a secondary study based on the model of usable security published by Whitten and Tygar (1999) in the first year of the SOUPS Conference (Garfinkel et al. 2005). The researchers proposed that it was not the usability of the system that caused security errors, but it was a problem caused by the backend of the system not seamlessly supporting security needs. They found that the use of a more usable interface plus a better back-end encryption system did enable fewer security errors to be made, but it still did not fix all the problems. They found that there were sociological problems of making trusting decisions that would influence security outcomes. For example, a user might get an email from a friend with a different, unverified email address. The question is do they trust them or not? They concluded that issues of trust are a problem that perhaps technology cannot fully address.

Hitchings published a paper that summarized and outlined the work up to that point, and that made the argument that there is a human side to security. He explained that, along with the technical side of security, there are human problems: the personnel having individual objectives, culture, and attitudes; the organizational problems such as policies; and context or environmental problems such as outside competitors or customers. These problems all will affect the practice of security. He concludes that, "The methods for implementing security are outdated and a new methodology is required that takes into account the people problem" (Hitchings 1995).

Another foundational article to the field of usable security was published in 1999 in the Communications of the ACM, a magazine published by the largest computing organization, which built off the work of Hutchings and raised the visibility of the emerging field of usable security. This article by Adams and Sasse (1999) provided a wide argument for how password security has to work with user practice to create usable solutions to privacy problems. Through the surveying of 139 users and 30 interviews, the researchers were able to derive four factors that affect how people use passwords, the last two highlighting how work practices are important: (1) multiple passwords, (2) password content, (3) the perceived compatibility with a user's work practices, and (4) the user's perceptions of organizational security and information sensitivity. Adams and Sasse explain that the lack of communication with the security staff along with a wrong mental model of how security works both influenced the user behavior: "Users perceive their behavior to be caused by a mechanism design to increase security" (McKnight et al.). By highlighting the incongruent practices of current security measures with user password

behaviors this paper provided a clear demonstration of how security as a field needed to evolve.

These papers highlighted how usable security emerged as a field that recognizes the balance conjunction of people and technology to respond to security needs. Not only did the field of security move beyond trying to solidify more rigid and rigorous rules to explore the human side, but they also started to utilize methods from the social science fields (i.e., interviews and observations).

### **2.1.2 The Social Side of Security**

Part of recognizing the human side of security is recognizing that systems of interaction are socio-technical. “Socio-technical” means that people, technology, and the surrounding context are all parts of a system of interaction that frame the practice of work (Flechais et al. 2005). In the recent work of usable security, researchers have published on how security is and should be designed as one part in the larger socio-technical system. The papers in this section extend beyond stating that security needs to be more usable, but also consider what aspects of the context and user are important for security.

The first piece of work by Flechais, Reiglesberger, and Sasse explored how and why examining security as one part of the larger socio-technical system can provide insight into how to create better systems. They emphasize the importance of defining security by its perceived vulnerability: “A computer is secure if you can depend on it and its software to behave as you expect. ... Dependability is therefore determined by the degree to which this socio-technical system behaves in a way it’s expected to” (Flechais et al. 2005). By highlighting the perceived dependability, the authors emphasized the user’s part in security. The researchers went on to explain how removing the human aspect of security could be dangerous. Humans are flexible, have intuition, and evolve. Computers systems, on the other hand, are rigid and less able to adapt to unstructured events. When used in combination, it is possible to create a reliable and flexible system of security.

Adams and Blandford (2005a) explored the clinical domain primarily to try to determine the factors that affected information and technology usage. Their secondary purpose was to explore the security and privacy problems that affected use without the “bias” of having a structured research question (a process that I am adopting). They demonstrate that the culture of the work setting influenced the types of security problems identified and also the resulting solutions. Their key findings were (1) that communities that did not adopt new security procedures circumvented security policies, (2) security mechanisms were sometimes purposed by people within the community to enforce power relations, and (3) when IT personnel engaged with the community they were more likely to create solutions that benefited the whole socio-technical system.

A few additional theoretical points from this paper are important to mention. First, Adams and Blandford make the argument that security, privacy, and trust have all been designed for the individual with little consideration for how to design for the group. This assertion supports my exploration of how communities manage these constructs in practice which is in contrast to other work that focuses the prototypical behind-a-desk

user. Second, Adams and Blandford use Communities of Practice as their theoretical underpinning to understand how groups interact. The emphasis on communities and work practice in this research are models for my own work.

In 2006 Dourish and Anderson published a position paper that directly examined security as a social process (2006). They argue that work within usable security has fallen traditionally within three areas: (1) empirical examinations of security practice, (2) empirical studies of the usability of current security systems, and (3) novel systems that have been designed to better support end-user security. From these areas of work on usable security a “narrow” view of security and privacy emerged, with the terms at times being used synonymously. Dourish and Anderson argue that models of security and privacy have to be valued as “practical, *ad hoc*, in-the-moment accomplishments of social actors, achieved through their concerted actions in actual settings” (pp. 328). They discuss new models of security and privacy to show how the study of work practice can, and should be, valued in this research. This call for a contextual and holistic analysis of security practices demonstrates the need for my proposed work.

To better understand the relationship between the social and technical side of security, work from Carayon (2006) has applied the dimensions of a socio-technical system model to network security concerns and health care. These dimensions vary by definition, but include aspects of the social system, the technical system, organizational structure and policies, contextual and environmental factors, and the current task. The socio-technical system model allowed for the researchers to understand how the system could be designed for all users to create safe practices, which is adopted for this dissertation. This is because, by using a socio-technical framework, other aspects of security and healthcare can be brought to the forefront. For example, in the realm of security, humans may represent the weakest link in a completely secure technical system. However, the social aspects of human may also account for flaws or gaps in current technical security systems. This is a similar argument presented by others, e.g., Flexhais et al. (2005). From the realm of health care, the increasing use of outpatient care is enabled through the patients co-producing their care through technology- and human-based support systems.

## **2.2 Privacy**

The personal information in childcare centers and physicians’ offices is sensitive. Sensitive means that the personal information has limitations delineating who should access it. I have adopted the definition from Nissenbaum that the terms “sensitive” and “confidential” in reference to personal information specify special information that denotes a need for privacy (Nissenbaum 2004). In the context of the information-rich environments I will be studying, a child or a patient’s information includes practical pieces of information that should be secured from a legal point of view, like social security numbers and consent forms, but it also contains social information, like a parent’s divorce or a medical diagnosis. Security mechanisms are the tools that will allow information to be made private.

The ownership of personal information is an important consideration in terms of privacy. Who owns the file being stored at the childcare center and the physician’s office? The file

contains information about the patient; it is their personal information. At the same time the information is written on the physicians' office's forms, annotated by staff, and used regularly by the physician's office. Personal conceptions of who owns the file or other copies of the personal information are going to affect the management of its privacy. This is especially true given the lack of an over-arching government regulation specifying rules about who owns that information. For instance, if the director believes that they are merely stewards of the personal information, they are going to restrict inter-office access to personal information based on the patient's request. In contrast, if the director believes that the personal information is the company's property, the personnel may share personal information regardless of what the customer desires.

Given the varying definitions of privacy, how information is protected is going to vary by individual and organization. This, in turn, can lead to breakdowns surrounding how privacy is instantiated into rules. For example, what is individually believed to be private may be in conflict to what an organization has stipulated as private. With the increasing emergence of electronic records, there additionally may not be policies yet created for how private information should be handled. Therefore, given these constraints in the socio-technical system and my previously presented research questions, I present an analysis of the construct of privacy.

### **2.2.1 Models of Privacy**

In understanding how privacy is a larger societal norm, Adams and Blandford argued that there are problems with the security of personal information. They explain that security mechanisms embody the cultural idea of personal identity. From the idea of personal identity stems personal information which then needs to be made private. They explain that, "The problem with many definitions of *personal information* is that they concentrate on the data itself rather than how it is perceived" (original emphasis, Adams et al. 2005a, p.178). Information is only private because there is a public space and the delineation between those two spaces are going to vary depending on an individual's relationship to the greater society or contextual situation (Harper et al. 1992). In tandem with this idea of boundaries is the concept of social identity. The concept of social identity is that the user has a public persona within a public space. The social identity is created through the divulgence of personal information that is then interpreted by others. Therefore, users have a need to conceptualize the personal information that they place in the public sphere (Bylund et al. 2008). The interplay between the personal and public identities is a dynamic negotiation between being hidden and being seen.

Palen & Dourish suggest a similar framework by building off of the work Altman to understand how the interconnections between technology and society create boundary situations where privacy is a concern (Palen et al. 2003). Altman proposes that privacy is a dialectic and dynamic boundary regulation process that is not rule-bound. Instead, there is a spectrum where peoples' accessibility is more open or closed. To build from Altman's work, Palen & Dourish propose genres of disclosure. Genres of disclosure are socially constructed patterns of interpersonal privacy management "that reflect, reproduce and engender social expectations, guide the interpretability of action, and evolve as both technologies and social practices change" (pp. 133). In practice, this

means that there are social boundaries on which technology will encroach on norms of privacy. Norms will then be established for how to manage accessibility to private information in these new situations.

While this model of social boundaries is thin, Dourish and Anderson suggest an alternative model of navigating information sharing called “cultures of secrecy” (Dourish et al. 2006). A culture of security is one in which groups ascribe meaning to certain pieces of information, thereby making them private properties. Because secrets afford intimacy, the sharing of secrets is a site of negotiation where people discuss, navigate, and redefine the social norms of what should be shared to whom, and under what circumstances. These norms are then used to structure the culture for new members and to mark group membership. This allows new members to learn what information is to be shared and discussed and outsiders.

An additional model of privacy is the economic exchange model. In this model, the user of a service is willing to give up some of their private information to gain that service. An example is the use of a frequent buyer card at the grocery store: the consumer provides personal information about goods purchased in order to receive product discounts. A problem with this model is that there is an implicit assumption that the user is rational. This assumption is similar to one made about participants in the prisoner’s dilemma game (Dourish et al. 2006). As Dourish and Anderson explain, studies of users in actual practice show that users do not always behave in a rational economic manner. A second problem is that this model does not reflect the social nature of privacy. “Privacy is not simply a way that information is managed, but how social relations are managed” (pp. 327). Just because a user behaves a certain way in a lab setting does not mean they can and will behave that way in their day-to-day lives. Instead, a person may exchange a piece of information for a service at one time with a friend to establish trust and interdependence. The one-to-one model of a user providing personal information for services does not necessarily account for the dynamic interplay of social relations.

Agre has also distinguished between two models of privacy (Agre 1994). He first asserts that privacy is a social construct. As new technologies are developed with novel methods of tracking people, their work, and their information, people think culturally about how their privacy is being managed. He argues that different models of privacy and data management highlight what are the different privacy concerns. One model that he examines is the surveillance model. The surveillance model embodies the ideas of watching, territorial spaces, and big brother style centralizing files. While this model highlights the possible negative aspects of aggregating information, it also highlights the associated fears. A different model proposed by Agre is the capture model. Agre explains that through the use of linguistic metaphors and the focus on local practice and activity reconstruction, the capture model highlights how the capturing of information enables communities to coordinate their work. The capture model focuses on creating ontologies of activities. While I am adopting neither of these models, they both highlight important aspects of how to conceptualize space of social privacy.

Nissenbaum conceptualizes privacy from how societies have made privacy norms into laws (Nissenbaum 2004). Three principles embody privacy: (1) the need to protect privacy against government intrusion, which is similar to Agre's concept of surveillance model (Agre 1994); (2) determining the spectrum what is sensitive, intimate, and confidential, which is similar to the economic exchange model discussed above; and, (3) determining the spaces and boundaries of where there is a public and private sphere (Bylund et al. 2008). The problem with these three principles, as argued by Nissenbaum, is that they fail to take into account the larger guiding principle of contextual integrity. The concept of contextual integrity is guided by the social norm of appropriateness, distribution, information flow, and change.

### 2.2.2 Designing for Privacy

Bellotti and Sellen (1993) considered how information technology facilitates new fantastic data manipulation and presentation. Two problems can arise in these new areas. The first problem is that these new information systems present novel vulnerabilities with untested protection mechanism. They quote Mullender in saying that "protection mechanisms 'are often only secure in principle. They are rarely secure *in practice*'" (original emphasis, 1993, p.1). The second class of problems, which are the ones that they focus on, are the design problems that disrupt and cause breakdowns in social behavior. When people are working together and communicating through mediating computer systems people can display more information than may be desired or they may oversee some information about a collaborator that they did not desire to see. In this sense they define privacy "to be a personal notion shaped by culturally determined expectations and perceptions about one's environment." Privacy is shaped by what are the cultural norms of the situation to determine what is acceptable. To design for privacy, Bellotti and Sellen propose a design framework of a 2 by 4 framework that considers feedback and control versus the aspects of capture, construction, accessibility, and purposes. Sasse and Blandford criticize this work by saying that there is a large assumption that designers can *a priori* know all of the aspects that a user would identify as a privacy invasion (Adams et al. 2005a).

In similar work, researchers explored the question of how to design file-sharing software that encourages participation while protecting privacy. The outcome was four usability heuristics on how users understand P2P file sharing software (Good et al. 2003). While similar to that of the original definition of usable security outlined by Whitten and Tygar (Whitten et al. 1999), the framework was conceptualized to be specific to privacy. The framework explains that P2P software is "safe" and "usable" if users (1) know what is being shared, (2) know how to share and not share, (3) do not share information that is overly sensitive or "dangerous," and (4) are confident that the system is not misusing their information (i.e., that it is trustworthy). Good and Krekelberg did multiple small studies examining how users inadvertently share personal information through the P2P file-sharing network KaZaA. While this study assumed that all users are rational and do not desire to share their personal information unnecessarily, they found that over a 12-hour period, 156 KaZaA users shared their email boxes. Among the four design aspects to respect privacy in P2P software outlined above, KaZaA failed all of them in user testing.

The work of Hong et al. proposed a model of privacy that can be applied to understanding the design space of future technology. They argue that privacy is “heterogeneous, fluid, and malleable notion with a range of needs and trust levels” (Hong et al. 2004, p.92). They additionally argued that understanding security mechanisms that attempt to regulate privacy are “by no means sufficient.” This is because security, if focused on protecting against adversaries, instead of on understanding contextual needs of individuals, cannot account for all factors. For their model they propose examining various aspects of the social and organization context, along with looking at the technical needs, by asking questions about the current design space. They specify that this method is different from those presented by Bellotti and Sellen (1993), and others covered in this review, because their work is practical and concrete. Example questions that the designer is to ask to herself are, “Who is the user of this system,” “How is personal information collected,” and, “How much information is shared”.

Another side of designing for privacy considers how to use sensors to detect the context of the situation that people are in, and thereby activate appropriate privacy settings. An example would be if a person was looking at their medical files on a public computer and a sensor detected an approaching unknown person. By detecting that someone else is present, the computer would enact a privacy protocol to remove the visibility of the screen until the unknown person passed. Sample scenarios can be seen in the work of Ackerman, Darrell, and Weitzner (Ackerman et al. 2001). They explore four usage scenarios of people interacting and the dimensions of privacy that should be considered (i.e., user controlled protocol enactment, secondary usage of the data, and user knowledge of sensors).

### **2.2.3 Software Designed for Privacy**

In the fields of usable security and human-computer interaction there has been work to create software that helps user think about their privacy concerns. One example of this kind of privacy software is visualizing parts privacy statements at pertinent moments (Egelman et al. 2009). Another version of this work involves the use of “privacy critics.” The privacy critics software uses pop-up windows to help prompt users think about the implications for divulging personal information (Ackerman et al. 1999).

Technology probes have been used in the work of Bylund, Höök, and Pommeranz (2008) to explore the effects of displaying personal information in an unusual places or with a unique methods. They were also used to display personal information through novel information and communication technologies. This work was fueled by the idea to explore how people balance their personal and social identities. Bylund et al. found that, while privacy concerns were high prior to the probe being deployed, participants were generally more engaged in the “creative playfulness” that took over after the deployment. This work highlights that privacy concerns and software should not primarily focus on how help users hide their information, but think more about how disclosure plays a part in social identity.

The work of Heckle and Lutters examined one software-based mechanism to provide privacy for hospital workers (Heckle et al. 2007). Their argument is based on the application of HIPAA to the workplace, which enforces that passwords can no longer be shared. To balance the need for security and privacy, they suggest the use of single sign-on authentication. Single sign-on authentication involves one user logging into a system. The system's network then manages that user's access to related systems as they work. Heckle and Lutters found that participants were particularly hesitant about having their email available through single sign-on authentication, that participants were likely to share workstations even with a different person logged in, and that participants were concerned about surveillance.

#### **2.2.4 Evaluations of User Privacy**

The use of privacy statements became increasingly ubiquitous in the design of software. The work of Arcand et al. (2007) therefore explored how modified privacy statements could encourage participant thoughts of control and trust in e-commerce websites. They found that privacy statements did make participants feel more in control of how their personal information was to be managed. However, whether the policy was opt-in or opt-out caused feelings of control and trust to increase and decrease, respectively.

Harper et al. conducted ethnographic work to examine the sociological implications for two labs using active badges to track location information. Active badges are badges that have chips and software built in to interact with the devices and network. Harper et al. argue that it is important to consider the sociology of the workplace to understand how the information will be used and how the workers will regard its use. In particular, they found that the role of the person in the organization, the information that was being tracked, and the users attitude all had a large impact on their use (e.g., a manager had different views than a non-manager. The responsibilities that the person's role also "includes what they feel a sense of obligation to do and a tacit, informally managed awareness of the need to co-operate with fellow workers" (Harper et al. 1992, p.349).

### ***2.3 Relevant Studies of the Management of Sensitive Information***

#### **2.3.1 Articulation Work**

How do you know that the work others say that they are doing is what they are actually doing? Part of the trouble with electronic systems and their design is that they attempt to articulate all of the work that people do for a myriad of purposes: to support collaboration, to support shared awareness, to support and predict for the tasks of an individual user, and more. The question for how to then support all of the details of various work practices is a uniquely wicked problem, with the term "wicked" stemming from the work of Rittel (Rittel 1972). For this reason, researchers have explored articulation work, which is a representation and accounting of shared work among a set of collaborators (Schmidt et al. 1996). More commonly articulation work has been purposed for understanding the work flows of organizations, but more theoretically stems from a desire to understand the work that people do. For example, articulation work has been used by Schmidt and Simone to evaluate the use of coordination mechanisms, which involves understanding how "cooperating actors devise and use coordinative constructs

such as coordinative protocols and workflows and how such constructs are supported by artifacts” (1996, p.156). Anselm Strauss, one of the pioneers of Grounded Theory, is credited with his foundational article in 1988 which documented the role of articulation research in “work processes, types of work, and interactional processes” (pp. 163, Strauss 1988).

Articulation work is a valuable area of research to consider in relation to this dissertation because it is a guiding paradigm influencing research on privacy and security. For example, work in role-based authentication stipulates that if system administrators could only articulate who should have access to specific information than privacy and security could work properly, e.g., Ferraiolo (1992) and Choydhury (2007). However, as seen in this dissertation, work is more than articulation.

In healthcare most work could be considered articulation work. Articulation work consists of sharing information in various artifacts, documenting what has been done and what needs to be done, and distributing tasks (Bossen 2002). Because some of the information that is being articulated is sensitive, articulation work serves as a valuable area to consider in regards to how people manage the sensitive personal information of patients. Other papers tend to focus on “trajectories,” which focus on the mutual accountability of people as they engage in large socially constructed tasks (Aarts 2001; Reddy et al. 2006; Zhou et al. 2010). These trajectories can be temporal (Strauss et al. 1985), or spatial (Bossen 2002), but dictate the constraints and needs for people to engage in some goal-directed activity. In particular, the work of Aarts is a valuable example demonstrating that the trajectory of a physician is only one trajectory. He argues to really visualize all of the invisible work of the healthcare community, the trajectories of patients, and others is also valuable (Aarts 2001).

In the work of Cabitza et al. (2006) the researchers present a conceptual framework for evaluating the different groups that people belong to and how they articulate their work. In this work they present the concept of intra- and inter-system articulation work to situate their study of hospital wards within the broader realm of research on socio-technical systems. Similar concerns are relevant for my dissertation (e.g., focusing on larger system wide concerns, the role of collaboration, and shared tasks). However, their work looks at boundaries where invisible work is not accounted for when sharing patients and work. Additionally, this work represents a continuation in the debate over paper versus electronic records and how these forms are relevant for sharing client information. Again, while valuable, this is not the concern of this work.

Other relevant work involves designing for increased patient agency in articulation work (Hillgren et al. 2006) and designing to account for the competence of healthcare workers (Larsen et al. 2008). These two pieces of research demonstrate issues, like patient agency and competence, which are relevant to the work, and should be considered in the design of any socio-technical system.

The work presented in this dissertation is not focused on articulation. Articulation, like Grounded Theory, focuses on the process and the coordination that focuses on artifacts,

movement, and flow (e.g., the work of Bossen 2002 serves as a valuable example). My work, instead, focuses on the embodiment and experience of security and privacy. However, the process and organizational policies can and do have an influence on the phenomenon of security and privacy, and are discussed in Section 4.9 and Section 5.1.2.1.

### **2.3.2 Abstract Places & Spaces**

A space is a three-dimensional location with physical qualities such as relational orientation, proximity, partitioning, and presence. What makes a space into a location that has meaning, or a “place,” is socially co-constructed values and behaviors that the space affords. For example, when conceptualizing a door as an element of a space, it functions as a partition and a divider of two spaces. When viewed as a place, the door affords privacy (Harrison et al. 1996). Places are created by people, events, and circumstances (Harrison et al. 2008).

The concepts of place and space are of particular importance when considering childcare centers and physicians’ offices. At a basic level this is because they are more than the physical space. They are places of caring, business, and healing. The door to the office at a physician’s office is imbued with the meaning of entering a room where you wait for your turn with the doctor. In terms of security, the office of the manager is a place where the patients’ files are stored, managed, and accessed with appropriate permission.

Harrison & Dourish have considered problems of privacy in terms of place and space (Harrison et al. 1996). They explain the concept of privacy is place-centric. By this they mean that privacy concerns vary by the meaning that has been ascribed to a physical location, such as the bedroom or the living room. This distinction is more than just a delineation between public and private spheres: “Places are constructed not only out of spaces, but also by the people present, and the events occurring in them” (Harrison et al. 2008, p.101). The places have meanings that have been previously and are continually socially constructed. For instance, what is permitted as possible for discussion in the living room of one family may be different than another and may be different again depending on the context of the situation, e.g., party vs. working on homework.

Understanding and studying places that have already constructed their conceptions of privacy, such as those that are being proposed for study, is critical when considering the design space for future technical interventions.

### **2.3.3 Physicians’ Offices**

There has been work outside of the sphere of research that has examined security concerns in the medical arena. One key example comes from the Agency for Healthcare Research and Quality, which has put together a tool kit specifically for examining security in the medical setting (2010b). This tool kit includes a set of scenarios that have depicted different circumstances that security and privacy concerns are embodied within. These scenarios are then disseminated to states and towns nationwide to encourage discussion. The AHRQ also has put together a document of business practices relating to security and privacy. These practices are divided into technical means of addressing

security concerns, but also the physical and people oriented means of addressing security. Example electronic business practices are the use of keycards and digital signatures. Examples from the “paper environment” are organizational policies and procedures. This tool kit is a demonstration of a growing trend in the recognition that both people and technology can play a part in the security and privacy of patient information. However, these documents are also an indicator that there is confusion about how to balance and manage the security of a socio-technical system in practice.

There has been ethnographic work to examine how communities work together to manage a patient’s information. In the work of Reddy and Dourish (2002) they explore how nurses, doctors, and other medical staff in an intensive care unit coordinate through the use of rhythms. They argue that the management of the patients and their information is so tightly coupled that they are inseparable from the work being done: “Information is not a separate focus of concern, but is woven seamlessly into the work of the unit.” To understand how workers could manage with such integrated systems, Reedy and Dourish explored the idea of rhythms of work. Rhythms of work are the repeated temporal patterns of increases or decreases in work activity and information management. This lens facilitated understanding how medical workers would transfer, communicate, and manage the work that needed to be completed.

Jakob Bardram is perhaps one of the largest voices in the field of HCI, medical systems, and usable security. In one of his earliest papers he analyzed how medical work systems use plans to mediate their work through the lens of Activity Theory (Bardram 1997). Bardram proposed that medical work system designers and users have an intrinsic need to plan, and, in turn, to crystallize these plans into representational and mediating artifacts. However, medical work systems are still deeply contextual. He explains this by segregating plans, as a conceptual unit, into their different uses. For example, he explores plans as socially constructed, and used artifacts along with exploring them as records and means of dividing work. This conceptualization of plans is useful for understanding how they are represented in Activity Theory. For my research I will need to determine if and how security is a type of plan, and how important these plans are for managing actual security work.

One of Bardram’s largest pieces of work has been his ABC Framework (Bardram 2005), where he proposes to support the activities of medical teams with “simple, light-weight, versatile mechanisms” (Bardram 2005, p.166). He argues that the medical setting is one that is valuable for studying given the pervasive use of technology, but that it also involves a setting that is different from the typical workplace. The medical setting is one that involves *ad hoc* collaboration, mobility, interruptions, and an extreme focus on communication. To examine this space he proposes to study the following dimensions of activities: time and space, which is the managing work in different physical locations and at different times; task, which is the managing the collection of services; and, users, which is the managing of real-time and asynchronous collaboration with awareness information. In later work Bardram outlines the principles that underlie the ABC approach: activity-centered resource aggregation, activity suspension and resumption, activity roaming, activity sharing, and activity awareness (Bardram 2009b). Bardram’s

work on the ABC framework has been applied to context-aware computing (Bardram 2009a). The idea is to link on going user-created activities to location-based systems of activity (e.g., the system detecting that the doctor is approaching a patient and pulling up her file).

Work has been conducted to examine how the medical setting has managed the security of private information (Adams et al. 2005a), how articulation work supports collaboration in a medical setting (Bossen 2002), how to manage the mobility of medical collaboration (Bardram et al. 2005), and the use and creation of multiple surfaces to help collaboration and management. This last example includes a specific focus on supporting medical work (Bardram et al. 2009).

### **2.3.4 Childcare Centers**

There has been a considerable dearth of research examining the realm of childcare center facilities as information managers. However, there has been research from Kientz and Abowd on how to design a technical solution to handle the amount of information that has to be stored and managed about children. This work started as a qualitative inquiry using interviews that questioned how a network of caregivers managed the record-keeping process. This network of people involved childcare center workers, parents, extended family, and doctors. The researchers' central argument is that record keeping is an important process of documenting when children reach developmental milestone. This practice, however, is tedious (Kientz et al. 2007). Important findings from the study were that doctors were the most trusted source of information about a child's development. Doctors also supply information during visits, but parents usually have their hands full and forget relevant facts. This relationship between parents and doctor is key to understanding the conceptions that parents have about authoritative information. The second related finding indicates that parents have concerns about the privacy of information managed by secondary caregivers, like childcare centers or nannies. The outcome of this research is a series of design requirements (e.g., Take advantage of existing motivations).

Additionally, studies from Kientz have demonstrated prototypes for a system that supports the needs identified in the prior study (Kientz et al. 2007; Kientz et al. 2009b). This includes providing a multimedia and developmental milestone repository with interfaces to display how the child is progressing. This milestone repository could be software that is deployed on a home computer. Another choice was to create an all-inclusive device that records pictures and videos of the child demonstrating milestone progress. This prototyped system could also include toys with sensors built in to record when children play with them in such a way that a milestone has been met. While this work is in the same area as my dissertation research, and documents some of the same needs (i.e., mass amounts of information, data recording, etc.), it does not focus on the security and privacy of practice. Additionally, this work has focused on how parents manage the documentation. Instead, I am focusing on how childcare centers manage documentation, with parents' involvement only influencing privacy concerns.

In other related work Park et al. have conducted work supporting Kientz's findings about the difficulties of parents and healthcare providers to share information about a child's health (Park et al. 2009). Prior research found that parents have dynamic daily schedules, yet have technology that is inflexible to support their needs (Beech et al. 2003). For example, parents have difficulty documenting when an illness has been announced at a childcare center or to document recent vaccinations: they do not have the tools freely available or the documentation is sparse and distributed. The findings suggested a system that is distributed across childcare centers, physicians' offices, and a child's home that works with smart devices such as cell phones, thermometers, and medicine bottles to capture relevant information. This research is a relevant exploration of the design space, yet it neglects the security and privacy problems in collecting the information. My work will build off of this research to examine the social interconnections within documentation practices and managing that information.

## **2.4 Breakdowns**

Breakdowns are natural and occur in all systems of interaction and at different levels. They have been a key focus in HCI because, by studying where there are user errors, designs for software could be improved. Work on breakdowns stems the work on critical incidents from psychology. In Flanigan's foundational paper on the critical incident technique he defines the method's purpose as "collecting direct observations of human behavior in such a way as to facilitate their potential usefulness in solving practical problems and developing broad psychological principles" (Flanagan 1954, p.327). Breakdowns are a type of critical incident. Critical incidents do not necessarily reflect a time when there is turbulence, but times that may be interesting to study why users purchase or do not purchase items on an eCommerce website (Oldenburger et al. 2008).

Foundational early work on breakdowns comes from Ehn (1988), Petroski (1985), Polanyi (1966), Rittel (1972), and Simon (1996), where the research is focused on errors that users make in technology systems. One of the earliest works on errors in the interface comes from 1981, when they are termed "action slips" (Norman 1981) and were derived from the work of Freud. Action slips are the result of breakdowns in the mental processing of external stimuli. Using the terminology of the research, the cognitive user is examining a stimulus that "activates" the slip, the brain's "schemas" then enacts the slip, and the cognitive capacity of user is overloaded while multi-tasking. In this work, the metaphor of user-as-computer embodies the notions of inflexible stimulus-response pairing to environmental conditions. Once the cause of the breakdown is deduced and the user's mental schema fixed, action slips are "cured." This research on user errors still continues, with the focus of the research on frameworks for understanding the psychological functions. See Reason (1990) for detailed analysis.

A response to this conception of a user-as-computer produced the work on situated action. In this work breakdowns are less of a focus. Instead, situated action focuses on how people coordinate their emergent activities to constantly respond in situ to the presented contextual contingencies. The basic unit of analysis in situated action is the relationship between the actor and the environment (Nardi 1996). Thus, breakdowns occur when the user is forced to move from the seamless activity at hand to focus on the

operations of conducting the activity. For example, Winograd and Flores explain that breakdowns occur when objects that function *ready-at-hand* no longer function in that manner (Winograd et al. 1986). A hammer can work as an extension of a hand to knock in a nail. It is only when the hammer no longer functions to knock in the nail that a breakdown has occurred. This phenomenon is sometimes called moving to *present-at-hand*.

The concept of an external object functioning as an extension of the actor is similar to the concept of “functional organs.” Function organ is the term applied to an external concept or artifact that mediates the actor’s ability to function seamlessly with the context (Kaptelinin 1995).

An intrinsic problem with the situated action standpoint on breakdowns is that they focus on the individual user, and fail to account for how communities of people may encounter breakdowns. Breakdowns are also conceptualized as problems with the artifacts or tools of use instead of also examining conflicts in motivation, rules, or other external contingencies.

Breakdowns have been foundational to structuring and analyzing the phenomenon presented in this dissertation. I define a breakdown and discuss their use in Section 3.3.2.

#### **2.4.1 Research Utilizing Breakdowns as an Analytical Framework**

Studying breakdowns provides researchers with places where intervention can help. In terms of software design, breakdowns have been used to study particular situations where current technology does not meet the needs of the users. For example, in work on activity awareness, breakdowns were studied to understand places where collaborative software did not support group tasks (Convertino et al. 2004; Humphries et al. 2004). Breakdowns were first found from field studies of the use of groupware software. These breakdowns were categorized by factors such as tool use, tasks, situational, and group dynamics. A confederate and a participant then replicated the induced the breakdown from the field in the lab setting (Convertino et al. 2004).

The study of breakdowns is not only prevalent, but their use is also diverse. Breakdowns have also been used to study how communication across different technologies may be effected (Hancock et al. 2009), for understanding a user’s mental model (Sheeran 2000), and for understanding the problems in design processes (Guindon et al. 1988). In medical work literature they have been used to understand how teams coordinate their work flows (Kobayashi et al. 2005) and work trajectories (Ren et al. 2007).

Fischer makes perhaps the most eloquent argument for the importance of studying breakdowns. He argues that humans learn from their errors. When designers then consider errors in the process of design “breakdowns reveal to us the nature of our understanding, our practices, and our tools.” Fischer goes on to explain that “by providing opportunities for reflection and sources for discovery, (Bødker) function in a positive rather than negative way” (Fischer 1994). He explains that the designer can

never “design away” all problems that may cause a breakdown because the designer is not the one experiencing and living within the design environment. It is only through engaging with the community living within problem domain that a designer can engage with the tacit knowledge required to respond to the breakdown. In this sense, breakdowns actually provide a framework to engage with the community for and with design.

## **2.5 *Summary***

Research relevant to my dissertation spans the areas of usable security, privacy, and medical informatics. From these areas the need to study the collaborative management of sensitive information emerges along with a rich methodological and theoretical background is present. I build on this work to study privacy and security and situated and contextual constructs that are co-constructed in the day-to-day practices of childcare center and physicians’ office personnel. In particular, I use the definition of Palen and Dourish to contextualize privacy. This definition led me to ask research questions that have led to the use of activity theory, phenomenology, and scenarios.

### 3 Method

To study the collaborative management of sensitive information, I used qualitative inquiry to study childcare centers and physicians' offices in rural-serving southwest Virginia. This involved collecting interviews and observations. To study this topic I presented my research questions in my introduction.

Table 3. Research Questions

How do socio-technical systems that use sensitive personal information manage breakdowns surrounding the implicit and explicit rules of process	
Research Question 1	What breakdowns happen when the explicit and implicit rules are not followed?
Research Question 2	How are breakdowns accounted for, negotiated, and managed in socio-technical systems where sensitive personal information exists?
Research Question 3	What are the implicit and explicit rules surrounding how physicians' offices and childcare centers handle sensitive personal information?

The interviews and observation data were collected, and Activity Theory was used to parse the data down to a set of breakdowns. This set of breakdowns is presented as a response to Research Question 1 (a full list of all breakdowns is included in Appendix A), and a subset of the data as a response to Research Question 2 & 3 is presented in Chapter 4. The breakdowns were then analyzed using Phenomenology to understand the experience of security and privacy to account for how the practices that resulted in breakdowns are negotiated, managed and situated in the socio-technical system. This analysis is presented as the response to Research Question 2, the outcome of which is presented in Chapter 5. Last, to understand the larger influencing rules that surround the essence of security and privacy, scenarios were used to prototype and explain spectrums of problems to answer Research Question 3. These scenarios are presented as Chapter 6.

In this chapter I present a description of rural-serving childcare centers and physicians' offices in rural-serving southwest Virginia (Section 3.1). I then provide a description of how the data was collected (Section 3.2). Last, I present how the data was analyzed using Activity Theory, Phenomenology, and scenarios (Section 3.3).

All studies were IRB Approved through the Virginia Tech Institutional Review Board with protocol IDs 10-451, 09-777, 09-580, and 09-515.

#### 3.1 *Participants & Locations*

This section provides a description of the area and locations where this study took place. For my dissertation I studied childcare centers and physicians' offices. For the purpose of this dissertation I provide these definitions:

**Childcare center:** a facility where parents engage in a service agreement with a care giver to assume responsibility and provide supervision of the child for approximately five days a week – less than 24 hours in the day, barring sickness; hold more than two children under the age of 13; licensed by the Virginia Department of Social Services (adapted from Virginia Department of Social Services Website (2010a)).

**Physician’s Office:** a facility where patients engage in a service agreement with health care professionals to provide care, education, and treatment to the patient, usually less serious than to warrant a visit to the hospital emergency room; seen by appointment and during regular business hours (adapted from Virginia Board of Medicine Website (2006) and inclusive of practices as defined by HIPAA to include doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies (2010e)).

Each location represents a place where people balance the provision of care along with the management of sensitive personal information. This data was collected in southwest Virginia. This section documents and describes the geographical area that the studies took place in along with a description of childcare centers and physicians’ offices.

### **3.1.1 Rural & Urban Virginia**

All of the participants in the study were located in urban locations of Virginia, yet also served surrounding rural locations. This defines the location as “rural serving” meaning that the area is urban but a large portion of the services are used by the rural population.

The boundary between rural and urban is difficult to define. This is because of multitude of conflicting definitions of what it means to be “rural.” These definitions can be based on population density, aggregated household income, and demographic factors (Coburn et al. 2007). For example, the U.S. Census Bureau defines rural as, “All territory, population, and housing units located outside of urbanized areas and urban clusters. Urbanized areas include populations between 50,000, and urban clusters include populations between 2,500 and 50,000” people; whereas, the U.S. Office of Management and Budget bases their definition on an idea of a location be metropolitan: “A metropolitan area must contain one or more central counties with urbanized areas. Non-metropolitan counties are outside the boundaries of metropolitan areas and are subdivided into two types, metropolitan areas and noncore counties. Metropolitan areas are urban clusters of 10,000 or more persons” (2008). These definitions highlight how the conception of “rural” can differ by population size and the surrounding locations.

Rural-serving care providers have been found to have the following relevant characteristics (2008):

- Patients are more likely to be uninsured (20%).
- Patients are less likely to seek preventative care and medicine.
- Rural regions have fewer physicians and dentists per patient, with 10% of physicians in this area versus 25% of population.
- Infants and adolescent mortality, along with rates of obesity and tobacco use, are higher.

- 41% of local public health agencies reported funding to be their main challenged, compared to 26% of non-rural agencies.

Not only is the difference in care between rural and non-rural areas important for understanding the culture of the community, but also it is important for highlighting the different factors that may be documented and managed about a patients' care.

The delineation between rural and urban is also important because it affects critical aspects of the care relationship. For example, socio-economic status affects how much parents can pay their childcare center, and in turn, the kinds of supplies that childcare centers can provide (e.g., web camera services). Another example includes the digital divide or the prevalence of internet access that can provide basic access to online databases or data storage of patient records. These factors provide the backdrop for presenting the larger picture of what security and privacy means in these centers. The question is not do they want to use electronic systems, but focused on the constraints of the surrounding area and user demographics.

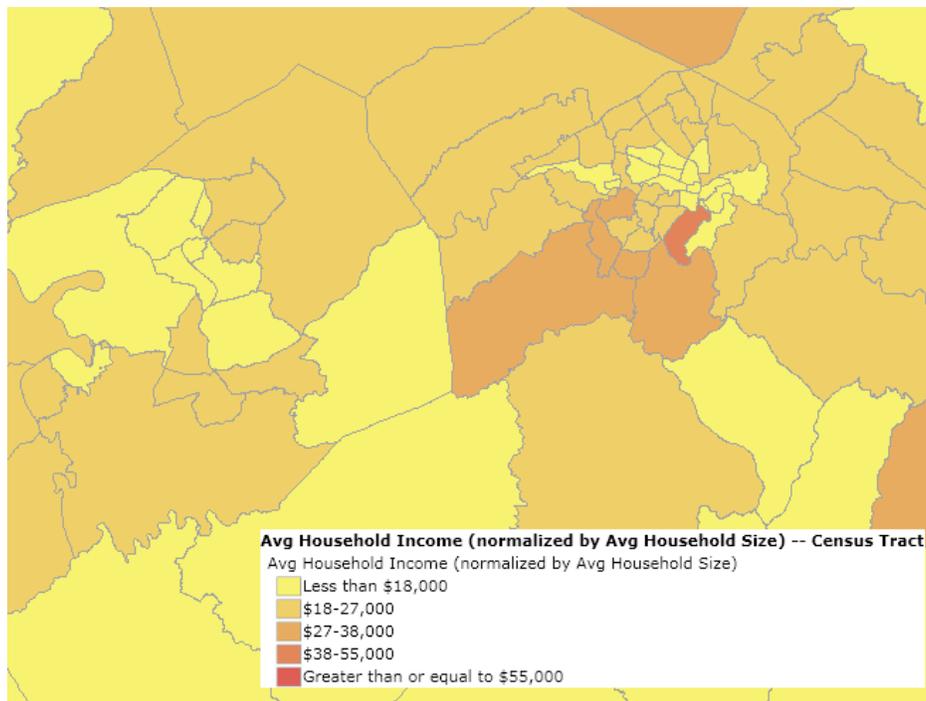


Figure 2. Map of average household income for the New River Valley, Virginia where the income is between less than \$18,000 and \$27,000.

The centers that were studied in this work are all located on the left-hand side of the map in Figure 2. The average income is between less than \$18,000 and \$27,000. The average monthly tuition for child care as of June 2009 for all childcare centers in the area was \$597.92 (min=\$460, max=\$815). The population of all of the studied counties and cities of Montgomery (89,193), Radford (6,447), and Floyd (7,404) equals to a little more than 100,000 people (U.S. Census Bureau, 2007b). For Montgomery County, where most of the studies took place, the population is 53% male, the median age is 26.6, 1.4% of the

people are of mixed race, and 89% of the population is white. One important point about Montgomery County is that the local universities, Virginia Tech and Radford University, heavily influence it. Virginia Tech hosts approximately 25,000 students who influence the community. The proximity of the centers in this study to the university also influenced the technology of the centers (e.g., one childcare center had a digital wait list system designed as a class project by students from the university).

The small-town nature of the locations that were studied can affect security and privacy. In these locations doctors will run into their patients in grocery stores, or a nurse will see that her friend's test result came back from the hospital. The strict distinction between friend and care provider can become blurred when your doctor also happens to be your neighbor and you serve on the same homeowners association board of directors. For instance, the pediatrician's office that was observed would see under-privileged children even though they knew that the parents could not pay for the services. They did this, in part, to serve the community and because the doctors were friends of the parents. Even though information about these special cases was shared with me, the particulars of the parents' financial circumstances was hidden from most of the people in the office to protect the privacy of that family.

A last point to make about the rural-serving centers that were studied is about the adoption of electronic records. There is a guiding assumption that electronic record systems will start to permeate these locations. However, these are places where not only is there a financial concern for the adoption of records, but also a social concern relating to people's fears of technology. Given the low socio-economic status of the clients, directors in the center report that cost is a huge problem for the adoption when they believe that their paper record systems are completely adequate. Second, there are fears surrounding the use of electronic records. The people in this study reported that they believe electronic systems will crash, that data will be lost, and that hackers will come in and steal all of the data. While these are real and valid concerns, they also highlight a lack of knowledge about how computer systems work thus affecting their adoption. The third factor influencing adoption in rural areas is the fears that the center staff echo from their patients. The staff talked candidly to me about how the doctors do not want to take tablet computers in to the receiving rooms when talking to patients. They worry about the client's fears of technology and they believed that this fear would then influence what the patients would then share with them.

### **3.1.2 Description of Childcare Centers**

Acceptance into daycares may be competitive; some centers have long waiting lists. One childcare center has a waitlist of at least four years for the infant and toddler rooms. In general, the cost of joining a waitlist is free. The amount of anxiety associated with this is represented by the fact that one childcare center offers parents the choice of paying \$100 to move to the top of the list. This stress may coerce parents into providing sensitive information in return for a chance of enrollment. The personal information that is generally stored on a waitlist is the birth date of the child, the parents' names, contact information, first date of contact, and representative notes. One location had an electronic waitlist. The remaining childcare centers had a physical hand-written notebook or

clipboard with lists of children who could be enrolled. In order to increase their chance of a child being accepted into a “good” childcare center, parents may have their child on numerous waitlists.

Most daycares have owners and/or boards of directors who are final arbiters of policy and management decisions. Policy decisions include problems such as how many times a baby’s diaper should be checked, cell phone usage in the classrooms, installation of new door locks, and the philosophy of childcare center. A childcare center philosophy is the approach to and interpretation of child development employed in fostering learning and growth. The philosophy is particularly important because it can foster how much documentation per child is completed to track the progress of children as they move through the developmental stages. Owners were found to have varying levels of involvement in the day-to-day responsibilities of the childcare center. For example, one owner divided her time between two different childcare centers. Another was more “comfortable” with the director and did not have “specific day-to-day responsibilities.” The board of directors can include parents, staff, and community members, and is concerned with the business as well as the conduct of the childcare center. For instance, one childcare center is part of a local church. Church members were included as part of the board of directors.

Owners and boards of directors have unlimited access to child and staff information. Yet, hands-off owners and boards of directors have little or no knowledge of the daily activities, the information that is stored in the environment, or the *in situ* negotiated security practices that are facilitating the highly coordinated work.



Figure 3. Pictures from different four childcare center directors' offices.

Running the day-to-day functions of the childcare center is a director who oversees the staff and child management. The director is a knowledge worker with management responsibilities. The director functions as a hub for day-to-day policy decisions, negotiations, and knowledge creation. She creates documents and spreadsheets, writes emails, and coordinates with the owners, board of directors, PTA, and licensors. The director is the public face of the business. She is the one who greets new parents who are interested in joining the childcare center, talks to parents when there are social and/or physical problems with children, and works with the waitlist.

Working in conjunction with the director can be other knowledge workers such as an assistant director, front-desk manager, and a receptionist. While not all childcare centers had these personnel, those that did used them in part to mitigate disruptions to the director. Often they responded to phone calls and greeted visitors. The administrative staff may also conduct information gathering for the director. Examples of this work include hourly calls to classrooms to check on the teacher-child ratio, monthly inspections of the facilities to make sure that individual rooms are compliant with DSS codes, or simply relaying messages of varying importance to and from the director to teachers.

The director's office and the adjoining spaces functions as a location for centralizing information about the children and staff. Typically, manila folders hold the most complete body of information about each child. These are stored in filing cabinets within a short walking distance of the director's desk. The childcare center directors and her office staff may have individual computers. Figure 1 shows the physical location of computers and filing cabinets in the offices of four different directors who participated in our study.

The classrooms are where the teachers and children spend the majority of their day. "Classroom" is the term used by the childcare center personnel; childcare center terminology borrows heavily from school terminology. In the classrooms, children have individual cubbies to store items brought from home, a central play area, counter space for documentation and also changing diapers. Rooms for older children have desks and tables to eat and work. Classrooms usually have individual names such as the "Blue Room" and are divided by age groups. For instance, children aged from four to six may be in the "Dolphin Room." Attached to each room can be an entrance to a general play area or to a smaller play area that is fenced. For example, children under two years of age may have individual play areas separate from the older children. Each room in the childcare center has a regulated ratio of teachers to children. An example ratio for an infant room may be one teacher for every four infants.

Classrooms store copies of information about children and original documentation. This includes contact information, allergy information, daily activity logs, progress logs and diaries documenting a child's developmental milestones, pictures of the children with their names, bathroom logs, and documentation of suspected abuse. In particular, stored in the cubby of each child can be notes, sometimes called "backpack mail," for parents, receipts, forms to be filled out and returned, and accident and incident reports.

Teachers generally function as go-betweens for parents and the director. Messages may be relayed through the cubbies, but important or sensitive information may be passed verbally through the teacher. Examples include payment information and changes in family structure. Parents work with the teachers to co-construct knowledge of a child's development by sharing information about daily progress at the start and end of each day. Within a classroom there is a lead teacher who dictates daily curriculum, communication with the director, and coordination with the cook. Teachers can participate in a parent-teacher association (PTA). When a PTA exists, its function is to meet and talk about fundraisers and concerns that may need to be addressed by the director.

Other people working within the childcare center may interact with sensitive information about the children. These include volunteers who move in and out of classrooms as they are needed or clean the workplace. Cooks also prepare daily meals for the children and have access to allergy information.

Many third-party services may become involved in the licensing of management in the childcare center. These services ensure compliance with laws and regulations. Compliance is important not only for the children, but also for the childcare center as a business and the communities' perceptions of the childcare center. The largest of these services is the Department of Social Services, a state run organization that polices the management of childcare centers through a licensing process. In Virginia, the DDS's reports are made available through a website housing detailed inspection reports. Other third party services and accreditation services are the NAEYC Accreditation Institution (2010c) and the Association for Christian Schools International, the public school systems for the early intervention of a child with special needs, doctors for information about immunizations and sometimes for physical and psychological care, fire marshals, the USDA, web camera services, web designers, accountants, and encompassing organizations that house the childcare center such as the Virginia Tech Research Department or Carilion Healthcare.

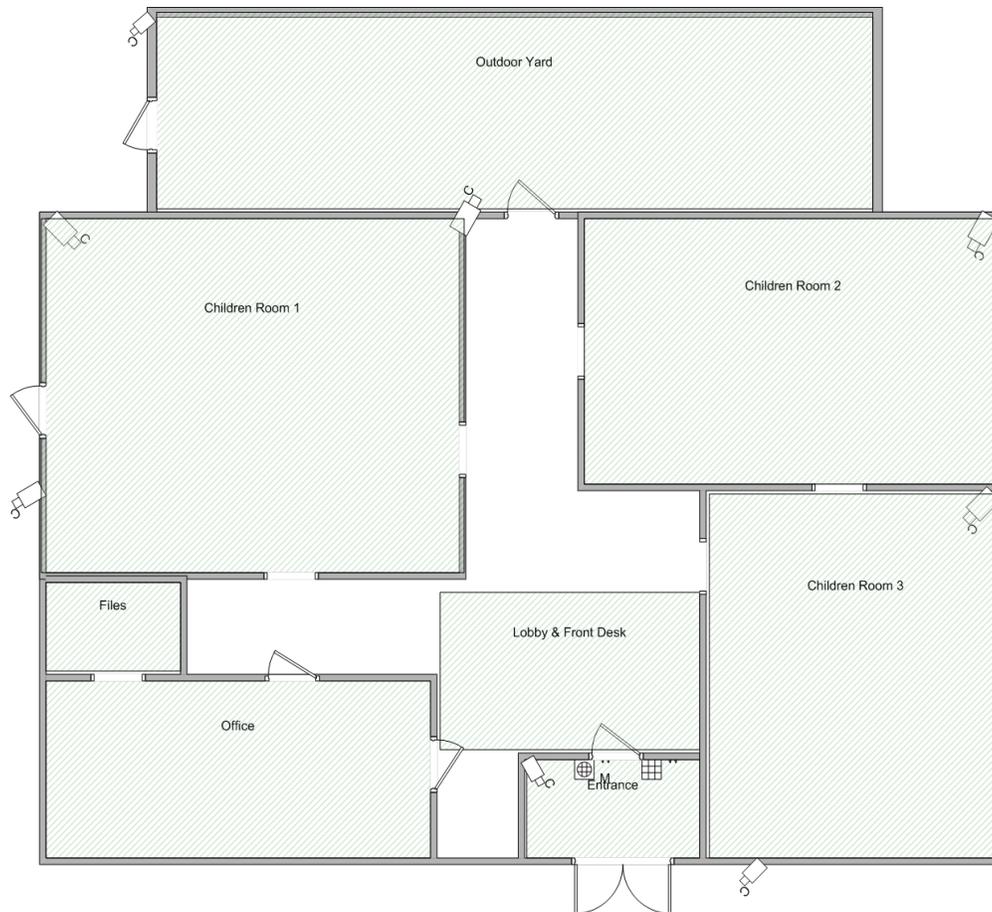


Figure 4. Sample floor plan for a childcare center.

Childcare centers have a typical physical layout, as shown in Figure 2. The front entrance is of particular importance. All childcare centers in our study emphasized an “open-door” policy through which anyone could enter the childcare during their open business hours. At a minimum, though, the childcare center have a bell to notify the presence of a visitor. In part, this is because of the variety of possible conditions surrounding access to the child. The childcare center has to be able to implement policies and make those policies work with their own needs. For example, if grandparents are to pick up children the childcare center providers need to make sure that the grandparents know the routine. Likewise, if the Department of Social Services needs access to the child or his/her information, the childcare center providers need to know that they are there and what their business is. Childcare center providers may also be asked to support legal arrangements that prevent a parent from seeing or taking a child.

Other childcare centers had even more security on their entrances. For example, researchers observed RFID badges, key pins, and buzzer systems. Upon entering the childcare center the visitor is usually greeted by the director or a receptionist. A sample picture of one childcare center entrance is shown in Figure 5. In Figure 5 the visitor enters from the right where they have been allowed to enter through the use of a buzzer-speaker system. The visitor is then greeted by the receptionist who is sitting behind the

wooden desk. In this greeting, the receptionist asks the visitor for her purpose in visiting the center. If the purpose is acceptable, then the visitor is asked to wait while the receptionist confers with the director. Parents may make payments with the receptionist and drop off any forms. After being greeted, parents will drop off their child in the appropriate room.



Figure 5. Front desk of a childcare center. There is a monitor and picture frame in the corner. Desk and 1-way mirror on the other corner behind (Branham et al. 2009).

Two childcares in our study had web camera system that could be used as an internal surveillance system for either security purposes or to watch teacher-child interaction. One of these also made their internal web camera system available to parents to watch remotely during the day. Parents logged into a website using unique passwords. The web-camera service allowed them to view common areas and the room that their child resided within during the day.

Childcare centers display information on walls, bulletin boards, and doors. As seen in Figure 5, even the desk of the receptionist is filled with information: there is a small red notice that is standing on two legs to let parents know about payment, there are flyers about swine flu, there is a digital photo album playing pictures of the children. There is also less explicit information: flowers indicate a subtle message about the place being one of growth and nurturing, Halloween spider webbing shows that it is a place of celebration and fun, and there is a hand sanitizing bottle that demonstrates that they are health conscious. Other information in the environment that is mandated includes food inspection reports, DSS licensing reports, notices of outbreaks of a sickness in a particular classroom, and fire marshal inspection reports.

Childcare centers are filled with a flurry of activity and then phases of calm. The busy phases usually are in the morning and afternoons when parents are dropping off and picking up their children. Other busy times include times prior to nap time and meal times. Calm times include nap time and pre-lunch. It is during the calm times that

teachers find time to document information about children and schedule meetings with other teachers in the center, parents, or the director.

Childcare centers are typically have a high percentage of female employees. In all of the childcare centers that participated in our study there were only two male directors and two male teachers. In one childcare center there was a new male teacher who was being hired and there was debate about whether or not he should be hired, even though he had good credentials. The female teachers expressed doubts as to whether or not he would actually change diapers, whether he would get frustrated easily, or if he would cause “drama” by dating any of the teachers.

### 3.1.3 Description of Physicians’ Offices

The physicians’ offices that participated in my study were selected as representatives of small independent rural offices that offered healthcare services. Physicians’ offices, which include doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies, account for 37% of the healthcare establishment (Niles 2010). A small physician’s office independently operates his or her own patient record system and schedule. The office is typically owned by the resident doctors, and the doctors serve as the central points of contact for final decisions. Again, similar to the childcare centers discussed in the previous section, the area is rural with patients traveling for some offices from surrounding states.

Almost all Americans are attended to through the American healthcare system. Most patients have health insurance through private or public insurance companies, but in 2006 15.8% of people did not have any form of insurance. Health insurance, in general, helps cover the expense of healthcare. In 2005 there were 1,169 million visits to physicians’ offices and outpatient care at hospitals with an average of 3.94 visits per person (Cutler 2008).



Figure 6. Displays of HIPPA regulation in physician’s office.

Physicians' offices rather than centers are licensed to make sure that they are complying with state and federal regulations. The largest and most prevalent federal policy is the Health Insurance Portability and Accountability Act (HIPAA) of 1996 that outlines privacy and security rules for managing a patient's health and financial information.

Figure 6 shows how one physicians' offices informs their patients of HIPAA regulations by displaying their policies in their waiting rooms. HIPAA is a broad yet influential policy that regulates processes for accessing information and also procedures for managing day-to-day aspects of information use. The Department of Health and Human Services explain on their website (2010e):

The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes. The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information.

Similar to childcare centers, the stakeholders for physicians' offices are made up of a multitude of people. These can be roughly divided into four different groups: patients and their friends and family, third-party stakeholders, healthcare providers, and non-medically trained office staff (Aita et al. 2001). Healthcare staff includes physicians, dentists, chiropractors, radiologists, nurses, nurse practitioners, medical assistants, and other medically trained professionals. Non-medically trained office staff includes receptionists, office assistants, office managers, file managers, schedulers, and directors. Patients include the person being seen and the patient's parents/families/guardians who can legally have access to patients' information. Third-party stakeholders that exchange information with physicians' offices include insurance companies, hospitals, pharmacies, referring doctors' offices (both referring and being referred to), laboratories, collection agencies, credit agencies (e.g., "Care Credit"), software companies, Medicare/Medicaid and lawyers (Vega et al. 2009a).

Front desk workers are usually the first people one encounters when entering a physician's office. These workers include receptionists, office managers, office assistants, file managers and schedulers. Front desk workers are generally responsible for scheduling appointments, printing the daily schedule for the doctors, handing forms to patients to sign and fill out, filing patient forms, filing and "pulling" patients' charts, filing insurance claims, billing patients, and keeping up with billing and insurance information. Front desk workers and doctors have the most access to patients' information. In some cases, office managers have more access because they deal with medical, schedule and billing information, whereas doctors in Study 1 reported having little contact with billing information. In addition to interacting with formal medical, schedule and billing information, occasionally, front desk workers reported informally

communicating information about patients to doctors, because they are the first people in the office to have contact with patients.

Medical offices are laid out in a similar fashion as childcare centers. There is usually a central entrance where the patient is greeted with a waiting room/lobby with access to a receptionist. The receptionist will note that the patient has arrived, and the patient will wait to be seen. The patient will then be guided back to a private room to be consulted with a nurse, and then a doctor. The patient's active files are usually stored around or behind the medical director's desk. Non-active files can be stored in a backroom and files that are even older can exist in a basement or in an external location.



Figure 7. A physician's office's files located on the surrounding walls of the director's office.

Files are organized by the patient's name, their last visit, and other relevant information as shown with the different color codes on the side. Patients can have electronic and paper files. There are sometimes separate files for billing and health information as well.

A last relationship that should be discussed is the relationship between physicians and pharmaceutical company representatives. Within a single three-hour observation four different pharmaceutical company representatives were observed to enter and talk with the attending physician. These representatives offer "lunch and learns" where the representative talks about their drugs and "teaches" about how it is beneficial. The aim is for the doctors at these locations to then prescribe that brand of the drug over other comparable drugs. Pharmaceutical companies have been reported to spend over 11 billion dollars a year on these promotional visits to offices and spend between \$8,000 and \$13,000 on each physician (Aggarwal 2010). This kind of spending and influence can have an effect on how information is managed. For instance, one pharmaceutical representative had an entire client's file faxed over to her office after a lunch-and-learn to see if that client could use the new device. In rural communities where the choice of any doctor is limited, the kind of influence and power that these representatives have is an important factor in considering how information and client care is managed.

To protect the identity of the participants a conscious decision was made to not provide descriptions of the locations that were studied. In town there are a very limited number of health providers who offer these services. Providing in depth descriptions would quickly identify the participants. However, for the purpose of provide some description, two of the physicians' offices managed care relating to teeth and gums, one on the care of children, and one on internal medicine.

### **3.1.4 Multi-site Fieldwork**

One of goals of phenomenology, the method of analysis used in this dissertation, is not to focus on one person or micro-culture, but to engage in discussion with varying aspects of the phenomenon to better understand its essence. However, beyond phenomenology, there is a history and even a growing trend in qualitative inquiry research methods to engage in multi-site study in order to do a breadth of study. Examples include the qualitative inquiry method of using case studies to conduct a deep study of many micro-cultures and to then explore the similarities and differences. Similarly, there has been an increase in the use of multi-site ethnographies such as the work of Marcus (1998), and within HCI Wyche's work serves as a valuable example (Wyche et al. 2009). Case studies, phenomenology, and multi-site ethnographies are really only instantiations of the same desire: to conduct fieldwork that engages in a broader spectrum of a culture or of a phenomenon.

To study the phenomenon of security and privacy within settings that manage sensitive client information two different types of locations were used. This is not to place value on the study of only childcare centers or only physicians' offices. Instead, this work represents an attempt to evaluate what both have as places that manage sensitive personal information. It is for this reason also that studying more than one of each type of location can add to the diversity of experiences being analyzed. In this sense, studying the experiences of 31 different locations adds to rigor of the study instead of detracting from the study.

In summary, my goal is not to study one culture one area, but to more broadly understand the experience of security and privacy of managing sensitive client information. This is better accomplished by gathering a spectrum of experiences

### **3.1.5 Participant Demographics**

This section details the participant demographics for all interviewed and observed participants. In total 21 parents were interviewed, 12 directors of childcare centers were interviewed, and 16 directors of childcare centers were interviewed. Of those who were interviewed, four childcare center directors allowed for follow-up observations, and two physicians' offices allowed for follow-up observations. An additional three physicians' offices were recruited for observations.



Figure 8. A visual representation of the different participant types.

### 3.1.5.1 Childcare Centers

The number of children being managed in the participating childcare centers ranged from 26 to 200 (sd = 63.7) with children ranging in age from six weeks to 12-years-old. The staff size at these facilities ranged from 9 to 45 (sd = 10.3). The average number of years of experience as a childcare center director was 12.6. In the entire surrounding area there are only two male childcare center directors/owners. One male director participated in our study. This fact reflects the particularly gendered community of childcare center workers.

Table 4. Characteristics of the participating childcare centers.

Location Identifier	Director's Experience (years)	Staff size	Child Enrollment	Date Interviewed	Title of Participant	Is Participant a Parent	Gender
Child-P01*	16	30	200	June 16th, 2009, October 13th, 2010	Director	No	Female
Child-P02	2.5	10	26	June 17th, 2009	Director	No	Female
Child-P03*	17	45	200	June 17th, 2009, October 8th, 2009	Director	No	Female
Child-P04*	20	15	43	June 18th, 2009, October 16th, 2010	Director	Yes	Female
Child-P05	10	11	40	June 19th, 2009	Assistant Director	Yes	Female
Child-P06*	15	22	100	June 19th, 2009, October 8th, 2009	Director	No	Female
Child-P07	0.66	24	86	June 22nd, 2009	Director	Yes	Female
Child-P08	4	23	145	June 23rd, 2009	Director	Yes	Female
Child-P09	18	9	40	June 23rd, 2009	Director	Yes	Female
Child-P10	22	24	27	June 26th, 2009	Director	Yes	Female
Child-P11	14	13	61	June 26th, 2009	Director/ Owner	No	Male
Child-P12	12	15	50	July 2nd, 2009	Assistant Director	Yes	Female
<b>avg</b>	12.59	20	84.83				
<b>max</b>	22	45	200				
<b>min</b>	0.66	9	26				

### 3.1.5.2 Parents

Eighteen women and three men were interviewed about managing their child(ren)'s information at childcare centers. The participants had on average 1.29 children, with the average age of the children being 4 years old. Nineteen of the participants had partners and two did not. The participants on average have had their children at their current childcare center for 14 month. Nine participants had used at least one childcare center.

Table 5. Demographic information for the parents who participated in our study.

Participant Identifier	Gender	Number of Children	Child(ren) age(s)	Partner	Current Childcare Center	Previous Childcare Center(s)	Time at Current Childcare Center (months)	Total Time in Childcare Center (months)	Date of Interview
Parent-00	Female	2	2.5 & 13 years	Yes	Child-P06	N/A	30	30	July 14, 2009
Parent-01	Male	1	3 years	Yes	External-1	N/A	18	18	September 14, 2009
Parent-02	Female	1	2.5 years	Yes	Child-1	Child-7	1	9	September 14, 2009
Parent-03	Female	1	9 months	Yes	Child-1	Child-12	1	9	September 15, 2009
Parent-04	Female	1	2.66 years	Yes	Child-1	Child-3	1	20	September 16, 2009
Parent-05	Female	1	4 years	Yes	Child-3	N/A	1	12	September 17, 2009
Parent-06	Female	1	1.33 years	Yes	Child-12	N/A	8	8	September 17, 2009
Parent-07	Male	1	2.5 years	No	Child-1	N/A	12	18	September 21, 2009
Parent-08	Female	1	3.5 years	Yes	External-2	N/A	41	39	September 22, 2009
Parent-09	Female	1	3 years	Yes	Child-1	Child-6, External-7	17	29	September 22, 2009
Parent-10	Male	2	3 & 7 years	Yes	External-2	N/A	17	29	September 25, 2009
Parent-11	Female	1	10.5 months	Yes	Child-6	Child-9	1	2	September 21, 2009
Parent-12	Female	1	2.5 years	No	External-3	External-8	24	29	September 22, 2009
Parent-13	Female	1	3	Yes	Child-1	Child-6	1	29	September 23, 2009
Parent-14	Female	2	2 & 4	Yes	External-4	N/A	18 & 17	18 & 17	September 24, 2009
Parent-15	Female	2	6 & 9 years	Yes	External-5	N/A	24	24	September 24, 2009
Parent-16	Female	1	2 & 5 years	Yes	External-6	N/A	15	15	September 24, 2009
Parent-17	Female	1	1.33 years	Yes	Childcare-1	N/A	1	1	September 24, 2009
Parent-18	Female	2	1.25 & 6 years	Yes	Childcare-6	External-9	2 & 48	2 & 62	September 29, 2009
Parent-19	Female	2	1.92 years	Yes	Childcare-6	N/A	1	4	September 29, 2009
Parent-20	Female	1	6 years	Yes	External-5	External-6	13	30	September 30, 2009

### 3.1.5.3 Physicians' Offices

Fifteen women and two men were interviewed about managing the sensitive information of patients. The participants had on average 20.16 years of experience as a director. The average staff size was 10 people with approximately 128 patients seen weekly.

Table 6. Characteristics of the participating physicians' offices, when the first contact or interview(s) took place, and the people who were interviewed. Asterisks indicate

participants who also were observed. Carrot indicates one participant who ran a center with doctors and supporting staff filtering through.

Location Identifier	Director's Experience (years)	Staff size	Number of Patients seen Weekly	First Contact/ Interview Date	Title of Participant	Gender
Med-P01*	35	8	120	June 30th, 2009	Director	Female
Med-P02	16	8	120	June 30th, 2009	Director	Female
Med-P03	5	6	65	June 30th, 2009	Director	Female
Med-P04	12	12	200	July 6th, 2009	Director	Female
Med-P05	16	21	400	July 8th, 2009	Director	Female
Med-P06	30	12	70	July 10th, 2009	Director	Female
Med-P07	4	9	65	July 10th, 2009	Director	Female
Med-P08	7	4	120	July 13th, 2009	Director	Female
Med-P09	18	3	70	July 14th, 2009	Director	Female
Med-P10	37	2	55	July 15th, 2009	Director	Female
Med-P11	21	6	75	July 21st, 2009	Director	Female
Med-P12	35	50 <sup>^</sup>	50	July 29th, 2009	Director	Male
Med-P13	2	2	100	July 31st, 2009	Director/Owner	Male
Med-P14*	N/A	4	N/A	July 6th, 2010	Director	Female
Med-P15*	5	10	70	July 1st, 2010	Director	Female
Med-P16*	20	7	60	July 13th, 2010	Director	Female
Med-P17*	35	17	200	July 13th, 2010	Director	Female
Med-P18	30	4	50	June 21st, 2010	Director	Female
Med-P19	35	10	250	July 24th, 2010	Director	Female
<b>avg</b>	20.16	10	128			
<b>max</b>	37	50	400			
<b>min</b>	2	2	50			

### 3.2 Data Collection in Childcare Centers and Physicians' Offices

Interviews and observations were conducted from Summer 2009 until Fall 2010 in childcare centers and physicians' offices. Part of this data and analysis was presented in the proposal defense, and for the purposes of the analysis presented in this dissertation is referred from here onwards as Study 1. All data collected after the proposal defense is referred to as Study 2. These definitions have been provided for clarification:

**Study 1:** All data and preliminary analysis of that data collected prior to the proposal defense. This includes all interviews with childcare center directors, initial observations of childcare centers, interviews with parents, and the first 13 interviews with physicians' office directors.

**Study 2:** All data collected post the research defense and analysis of all data from all studies. The data collected includes observations of childcare centers and physicians' office along with two additional interviews with physicians' office directors.

The data collected in Study 1 and Study 2 involved collecting interviews and observations, and creating and collecting relevant artifacts and is detailed in this section. The general outline of data collection involved the creation of a sampling method, designing interview and observation protocols, training, participant recruiting, training and preparation, conducting the interviews and observations, and then transcribing and collating the materials for data management.

### **3.2.1 Sampling Method**

A stratified criterion sampling was used. The goals of this sampling method are to illustrate subgroups that can provide comparison, along with providing some criteria for quality assurance. The first requirement for participating in the study was that the research participant has to have experience with security and privacy at a childcare center or physician's office. The second requirement is that the childcare center or physician's office must be located within the New River Valley, thus functioning as a representative of a rural-community serving business. The participants were also stratified so as to provide diverse experiences. The stratified groups were childcare centers, physicians' offices, or parents.

### **3.2.2 Protocols for Conducting Interviews & Observations**

#### **3.2.2.1 Conducting Interview Protocol**

The interview protocol was designed by three researchers and reviewed by one additional researcher. (Copies of all protocols are included in Appendix C.) There were four goals that divided the interview protocol into corresponding sections: (1) to collect background information about the center and the center director; (2) to induce the participant to think about and become familiar with speaking in regards to their information documentation, storage, communication, and access methods; (3) to itemize all of the stakeholders, knowledge sharing methods, and explicit information documentation; and, (4) to derive the participants concerns about the use of web-cameras, and electronic systems. Participants were provided a copy of a table that listed known stakeholders and possible communication methods. All questions were open ended (e.g., "How is access to information about children or other people managed?"). Researchers explicitly did not use the word "security" during the observation, although the participants did discuss the topic. This choice was to discourage participants from believing that the researcher was making a judgment about how secure their practices are. This practice has been used successfully in the work of Value-Centered Design to unravel the constructs and facets of dynamic concepts such as privacy (Friedman et al. 2002). The interview protocol was designed to facilitate asking follow-up questions or questions that were not on the protocol to expand on the themes of security.

Twenty-four hours before each interview the participant was contacted to verify the time and place of the interview. The place for directors was the center, but for parents the

location was either the participants work location or at a local coffee shop. The participant signed an informed consent form, and was reminded that they would be audio recorded. After each interview the researcher was given a brief tour of the facility. Pictures of the facilities along with representative artifacts, such as the forms that the clients fill out and return to the center, were collected.

The only participants that were paid for participant were parents. Parents were paid after the interview was conducted. They were paid \$10.00.

### 3.2.2.2 Conducting Observation Protocol

Observations were conducted in Study 1 and Study 2 using similar methods to generate and collect the data. For the people who participated in observations, they were presented with Informed Consent forms that were signed. Prior to signature participants were asked if they had any questions. They were told that we would not write any identifying information about children or patients, that all information would be kept private, and that all notes would be associated with a unique anonymous participant ID number. The participants asked no questions, but there were discussions during observations about what was being recorded. The observers stated that the participants could read any notes, and that identifying information was not being recorded.

Observations were conducted by shadowing the director, or when the director was not available, someone from the front office. Typical shadowing procedure was followed with observer keeping a running record, meaning that they kept a sequential record of occurring events, as described in (Bredenkamp et al. 1992). Shadowing is a technique developed to observe a particular person acting and interacting in their daily lives. This method allows the observer to attempt to see the participant's life through their eyes while being grounding their work in the particulars (Desjean-Perrotta 1998). The shadower follows one participant and details the actions that they take and the objects they interact with.

This decision to shadow the director was made for a many reasons. First, the front office is where the client's files were stored, accessed, modified, and where files were returned. Second, the observations are a method of triangulating the data from the interviews, which were with the center's directors. Third, many centers only used computers or other forms or technology in the front office for managing client information. Therefore, studying how client information is managed in a socio-technical system involved studying where the technology was primarily located. For these reasons observations were conducted primarily in the front office. However, there were times when the directors of the center had to leave their office or the front office to engage in some other task. If the observer had permission, then the researcher would continue to shadow the participant. There were times, for example when a parent requested a private parent-director conference, where permission was denied. At these times someone else in the office was shadowed or the researcher made general observations of the location for a short period.

The observer detailed most of what could be observed with time stamps approximately every 3-5 minutes. There were times when, given the space of the office, the observer was not able to watch all interactions on the director's computer monitor. In these times the observer would gently ask the participant what activity she was engaged in. The observer, when conflicted about what to write given the large amount of activity, focused on a number of factors:

- The activity of the director
- What current information people were looking at or for
- The location of any client information (e.g., the current state of the information space when we first enter the center)
- Any modifications or access made to client information
- Any verbal exchange of client information to other people in the center
- When the director engaged with technology
- Participant attitudes when sharing information

Given the previously provided definition of privacy as being situated and local, it was critical to not overly scope who or what was being observed. For this reason, whoever came into contact with the director or the person who was being observed was noted.

Observation notes were different dependent on the location because of IRB requirements. For childcare centers we were allowed to collect audio recordings and pictures. However, for studying physicians' offices, we were not allowed to annotate any identifying patient information, make audio recordings, or take pictures. Notes and hand-drawn sketches were the primary source of data for both locations. These notes were taken using either a laptop computer, or for the researchers less familiar with participant rapport, notebooks and pens. This choice was explicit because the use of technology in a location with a dearth of technology could influence how people interacted with the observer. Therefore, observers without demonstrated ability to build participant rapport, and thereby a disability to calm participants about the use of laptop as an instrument, used paper notes instead.

### **3.2.3 Participant Recruitment for Interviews & Observations**

Twelve childcare center directors and assistant directors participated in our first round of interviews. A comprehensive list of all licensed childcare centers in the surrounding area was collected using Virginia's Department of Social Services (VDSS) website. The VDSS website provides the latest and prior licensing information for each childcare center in the state of Virginia. In total, the website provided a list of twenty childcare centers in the area as of June 2009. Each childcare center was then contacted by phone and asked to participate in our study. Some places had to be contacted numerous times before a final decision was made as to whether to participate or not. Of the places that declined to participate, the reason given was that they were too busy to find time to be interviewed. When a director was contacted the pertinent information from the phone call was documented in a collaborative document shared with all researchers.

While the data from the interviews with childcare center directors was being analyzed, interviews with thirteen directors of physicians' offices were conducted. To recruit the

participants, two researchers worked to create a comprehensive list of all physicians' offices in the area using numerous online search engines. They then canvassed all of the physicians' offices in the area and added any additional ones that were not currently listed to notes. Also annotated was whether or not a person agreed to participate, whether or not the researchers should return, and if another office was recommended.

The researchers suspected that it would be more difficult to encourage participation in this study. To combat this fear we used a foot-in-the-door technique of visiting each place with a letter of introduction, a copy of our IRB approval letter, and business cards. We received three types of responses to our inquiries: no, they were not interested; maybe, they needed to check with their director and could they call us later; yes, for which they made an immediate appointment for us to return. All of the maybe responses later resolved to "no's" during follow-up phone conversations.

Parents were recruited using flyers in childcare centers, a list server for local working mothers, and a company newsletter. Participants contacted the experimenters by phone or email, and appointments were set up.

Participation in observations was more difficult. Initially all childcare centers that we contacted agreed to participate. However, as participation extended into the third, fourth, or sixth session, all but one participant showed hesitation to continue to participate. For this reason, the number of observations became limited. Participation by physicians' offices was even more difficult. It is the opinion of researchers that proximity to the university resulted in centers having a decreased desire to help with observations without monetary compensation (i.e., They were pestered often to participate in research studies without compensation). All interviewed participants were re-contacted, with only one agreeing to observations. New participants were recruited and the students found that, as the search for participants spread beyond the 5-mile radius, the number of participants agreeing to be interviewed or observed also increased. This resulted in one center agreeing to an interview, one center agreeing to an interview and observation, and three centers agreeing to observation.

### **3.2.4 Training & Preparing for Interviews & Observations**

To prepare for interviews with the childcare centers, an annotated bibliography of relevant literature was created that examined practices for community security management. The person who worked with me to conduct these interviews was an undergraduate researcher. For him to become familiar with interview methods, half-day training sessions occurred for one week with that used discussion, practice sessions, and readings on interview methods and best practices. Examples include Spradley (1979), Glesne (1992), and Suddaby (2006). I conducted the first interview by myself to become familiar with the interview protocol. I then conducted the second interview with the undergraduate student watching how I established participant rapport and used the interview protocol. The undergraduate student then conducted the third interview and I gave feedback and guidance afterwards. The undergraduate student conducted the fourth interview by himself, and I gave him feedback the same day after listening to the audio recording. This transitioning of the interviews allowed the scaffolding the

undergraduate's skills and training.

To collect the initial interviews with directors of physicians' offices I worked with a sociology student who was familiar with healthcare and interviewing. To prepare for the interviews the sociology student and I went through some preliminary results from the interviews from the childcare center directors and we talked about the relevant problems also in the medical settings. I read HIPAA and passed along relevant parts to my collaborator. In regard to her ability to conduct interviews, she had prior experiences with interview techniques (interviews and focus groups for her own dissertation), and felt comfortable with the interview protocol. We practiced the protocol and also read studies such as Reddy et al. (2006), Benotsch et al. (2004), and Kobayashi et al. (2005) to familiarize ourselves with methods and outcomes. The sociology student had three meetings with me to prepare, and one meeting with an additional researcher on the project. The scaffolding was conducted with this student with me attending the first two interviews. I also attended some subsequent interviews from interest, not because I did not trust the student's ability.

The protocol for conducting the interviews with the parents was similar. Two graduate students enrolled in a course taught at Virginia Tech worked with me to conduct these interviews. The researchers prepared for the interviews with the parents by reading the prior reports, transcripts from the initial interviews with the childcare center directors, related research, and practicing interview techniques. Two meetings focused on discussing the techniques of interviewing parents. Additionally, I attended the first five interviews to provide feedback after each session.

Similarly, while the interviews with parent were being conducted, follow-up interviews with childcare center directors were being conducted along with observations with two additional graduate students in the course. These researchers prepared for their interviews by working with the undergraduate student who had conducted the first round of interviews and me. Together we went over previous interviews and reports. Given the limited number of participants, practice interviews were not possible. However, I participated in all interviews to establish continuity from the previous research that summer.

To prepare for observations of physicians' offices a graduate researcher worked with an additional undergraduate student and to conduct the experiment. The undergraduate student underwent similar training as the prior students who worked with me. She spent a week reading prior interviews and reports, and read relevant literature about conducting observations and interviews. Both the graduate and undergraduate student conducted practice observations by watching and noting the actions of a knowledge worker. The students then received feedback.

Finally, I conducted a last round of observations in Fall 2010. All interview transcripts, forms, notes, diagrams, observations, pictures, and reports were reviewed prior to contacting participants.

### 3.2.5 Data Management

The data that was collected was sensitive. If the participant discussed practices that were not strictly up to code or if we observed practices that were against policy, these could be used for the centers to lose their licenses. Therefore, we went through a series of protection mechanisms to keep the data secure. First, all data was stored on a password protected computer, and unique participant identifiers were used when data was transferred from paper to electronic versions. Second, last names were never recorded. Third, all paper documentation (except for informed consents) was shredded once an electronic copy was made. If any identifying information was ever printed, it was stored in a locked filing cabinet. Together these mechanisms have kept the data protected.

All interview protocols are included in Appendix C. The general method to manage data was to assign a file by a unique identifier by the location and then if the data was specific to a particular identifier for that person. Dates were also included on files due to repeat interviews and numerous observations occurring at a single location. The interview transcripts, recordings, forms, pictures, and field notes were treated as the primary source of the data. The data, when memo'd, had the date listed in the text of the file. These memos were generally color coded to provide clear delineation between interpretation of the experience and the raw notes (except in cases when there was only one round of memoing). These notes were then aggregated first by participant and then by center in a file structure.



Figure 9. Sample of how memos were used to bracket interpretations and notes.

### 3.2.6 Dates & Times of Observations

Observations were collected in Study 1 and Study 2. The observations collected in Study 1 were only of childcare centers and is included in

Table 7.

Table 7. Dates and times of observations of childcare centers in Study 1.

<b>Participant Identifier</b>	<b>Dates of Observation</b>	<b>Time of Observation</b>	<b>Duration (hours)</b>
Child-P01	October 13th, 2009	3:00 PM - 5:45 PM	2.75
	October 14th, 2009	9:30 AM - 12:30 AM	3
	October 20th, 2009	3:00 PM	0
Child-P04	October 16th, 2009	2:00 PM - 4:00 PM	2
	October 26th, 2009	3:00 PM - 5:30 PM	2.5
	November 5th, 2009	12:00 PM	0
Child-P03	October 13th, 2009	7:30 AM - 10:00 AM	2.5
	October 15th, 2009	3:00 PM - 5:00 PM	2
	October 21st, 2009	10:00 AM - 12:00 PM	2
	October 30th, 2009	2:00 PM - 5:00 PM	3
Child-P6	October 22nd, 2009	12:30 PM - 3:30 PM	3
	October 23rd, 2009	2:00 PM - 5:00 PM	3
	October 29th, 2009	10:30 AM - 2:30 PM	4
<i>total</i>			29.75

Table 8. The dates and times of Study 2 observations with childcare center and physician's office directors.

<b>Participant Identifier</b>	<b>Dates of Observation</b>	<b>Time of Observation</b>	<b># of Observers</b>	<b>Duration (hours)</b>
Child-P01	August 31 <sup>st</sup> , 2010	12:00PM – 4:00PM	1	4
	September 2 <sup>nd</sup> , 2010	1:00PM – 4:00PM	1	3
	September 8 <sup>th</sup> , 2010	1:00PM – 4:00PM	1	3
Child-P04	September 8 <sup>th</sup> , 2010	7:45AM – 12:00PM	1	4.25
	September 14 <sup>th</sup> , 2010	11:00AM – 4:00PM	1	5
Child-P06	August 30th, 2010	12:00PM - 2:30PM	1	2.5
	September 2nd, 2010	9:15AM - 12:00PM	1	2.75
	September 9th, 2010	10:00AM - 12:45PM	1	4.75
	September 15th, 2010	9:00AM - 2:30PM	1	5.5
Med-P01	June 7th, 2010	8:15AM - 11:30AM	2	3.25
	August 20th, 2010	8:30AM - 11:30AM	1	3
	September 1st, 2010	8:30AM - 12:00PM	1	3.5
Med-P14	July 6th, 2010	9:15AM - 12:15PM	2	3
Med-P15	July 1st, 2010	9:00AM - 12:00PM	2	3
	August 16th, 2010	1:00PM – 4:00PM	1	3
	August 20th, 2010	1:00PM - 3:30PM	1	2.5
	August 26th, 2010	12:00PM - 5:00PM	1	5
Med-P16	July 13th, 2010	1:00PM – 4:00PM	2	3
	August 19th, 2010	1:00PM – 4:00PM	1	3
	September 7th, 2010	1:00PM - 4:15PM	1	3.25
	September 9th, 2010	1:00PM - 3:00PM	1	2
	Med-P17	July 15th, 2010	9:00AM - 12:00PM	2
Med-P17	August 19th, 2010	9:00AM - 12:00PM	1	3
	August 23rd, 2010	9:00AM - 11:30AM	1	2.5
<i>Total number of observed hours</i>				<b>96</b>

Observation times were purposefully chosen to span the times of the day that the centers that participated in my study were open. Childcare centers opened between 7:00AM and 8:00 AM and would remain open until 5:00PM and 6:00PM. Physicians' offices similarly opened between 8:00AM and 9:00AM and remain open until 5:00PM and 6:00PM, with some of them closing earlier because of the day of the week.

Table 9. The times of observations at childcare centers visually depicted to demonstrate that all times of the day were observed. Similar shades of blue indicate the same center.

	7 AM	8 AM	9 AM	10 AM	11 AM	12 AM	1 PM	2 PM	3 PM	4 PM	5 PM	6 PM
August 30th, 2010						Light Blue	Light Blue	Light Blue				
August 31st, 2010						Dark Blue						
October 13th, 2009									Dark Blue	Dark Blue	Dark Blue	Dark Blue
October 13th, 2009	Light Blue	Light Blue	Light Blue	Light Blue								
October 14th, 2009			Dark Blue	Dark Blue	Dark Blue	Dark Blue						
October 15th, 2009									Light Blue	Light Blue	Light Blue	
October 16th, 2009								Dark Blue	Dark Blue	Dark Blue		
October 21st, 2009				Light Blue	Light Blue	Light Blue						
October 22nd, 2009						Light Blue	Light Blue	Light Blue	Light Blue			
October 23rd, 2009							Light Blue	Light Blue	Light Blue	Light Blue		
October 26th, 2009									Dark Blue	Dark Blue	Dark Blue	
October 29th, 2009				Light Blue								
October 30th, 2009								Light Blue	Light Blue	Light Blue	Light Blue	
September 14th, 2010					Dark Blue							
September 15th, 2010			Light Blue									
September 2nd, 2010							Dark Blue	Dark Blue	Dark Blue	Dark Blue		
September 2nd, 2010			Light Blue	Light Blue	Light Blue	Light Blue						
September 8th, 2010							Dark Blue	Dark Blue	Dark Blue	Dark Blue		
September 8th, 2010	Dark Blue											
September 9th, 2010				Light Blue	Light Blue	Light Blue	Light Blue					

Table 10. The times of observations at physicians' offices visually depicted to demonstrate that all times of the day were observed.

	8 AM	9 AM	10 AM	11 AM	12 AM	1 PM	2 PM	3 PM	4 PM	5 PM
August 16th, 2010						█	█	█	█	
August 19th, 2010						█	█	█	█	
August 19th, 2010		█	█	█	█					
August 20th, 2010	█	█	█	█	█					
August 20th, 2010						█	█	█		
August 23rd, 2010		█	█	█	█					
August 26th, 2010					█	█	█	█	█	█
July 13th, 2010						█	█	█	█	
July 15th, 2010		█	█	█	█					
July 1st, 2010	█	█	█	█	█					
July 6th, 2010		█	█	█	█					
June 7th, 2010	█	█	█	█	█					
September 1st, 2010	█	█	█	█	█					
September 7th, 2010						█	█	█	█	█
September 9th, 2010						█	█	█		

### 3.2.7 Transcribing Data

The raw data for this study consists of the raw notes from interviews and observations, audio recordings, forms provided by the participants, and pictures. All interviews were transcribed with timestamps and notations of who was talking. Observation notes were additionally layered with explanation of ambiguous statements. These notes were bracketed and include personal reflections. Pictures and diagrams were also interlaced in these observations to explain anything that was being discussed. Data was then shared with at least one other researcher for clarification.

In total, the data that resulted from all interviews and observations is approximately 2,000 pages of transcribed data.

### 3.3 Data Analysis

Data analysis was conducted in three stages. The first stage involved using Activity Theory to isolate the breakdowns in the data. The second stage used Phenomenology to understand the experience of security and privacy. Last, scenarios were designed to respond to the breakdowns and in congruence with the analysis of the phenomenon of security and privacy. This analysis is presented in more detail in this section along with a description of the theory used.

### **3.3.1 Combining Data Across Study and Location**

All data from Study 1 and Study 2 along with data from childcare centers, physicians' offices, and parents have been combined and are considered the corpus of data to be analyzed. This decision was purposeful. First, both childcare centers and physicians' offices are two types of the broader category: locations that collaboratively manage sensitive information. Second, the purpose of this study is to provide information about this larger category. While the specifics of particular locations are valuable, and there are variations in the practices, the broader goal is to understand the phenomenon. Third, data from Study 1 and Study 2 was used even though there was a period of time between the start of the collection of data from Study 1 and the start of data collection of Study 2. However, this period of time between the end of one and the start of another was only 8 months. While there is a concern that during this time practices may have changed, contrasting cases are interesting, and reflect a breakdown had occurred in the system and thus serve as a point of study for this dissertation rather than as a problem. Indeed, contrasting cases is a goal of the phenomenological analysis of data, as presented in Chapter 5, to better convey the larger experience.

Careful precautions were made during the data analysis between at all stages of analysis to make sure that the data was not skewed towards either childcare centers or physicians' offices, or alternatively between Study 1 and Study 2. For instance, after all the breakdowns had been elicited, researchers annotated each breakdown as occurring in either Study 1 or Study 2 and then assessing if the data was more weighted towards the other. An unbalance could indicate that more data collection or analysis was necessary.

### **3.3.2 Activity Theory as a response to Research Question 1**

The first research question asked about what kind of breakdowns occur. Activity Theory was selected as a framework for eliciting the breakdowns from the data. Activity Theory offers a framework that is complementary to phenomenology, and has been demonstrated by others to be useful in understanding the conflicts that cause breakdowns. This section presents Activity Theory and how it can be used to explain breakdowns. It further defines a breakdown.

A description of the analysis to generate the list of breakdowns is included in Section 2.4.

#### **3.3.2.1 Activity Theory & Breakdowns**

Section 2.4 briefly covered the relevant history and literature related to the use of breakdowns to study how humans interact within socio-technical systems. For my research, the definition of a breakdown stems from the work of Fischer (1994) who presents breakdowns as opportunities within a larger design space. This definition is an optimistic one, not seeing a breakdown as merely another problem but as a place to engage the community for the design of future solutions. To document and evaluate the breakdowns a definition from Activity Theory Literature stemming from Engeström has been adopted (Engeström 1987; Kuutti 1995; Engeström et al. 1999; Barab et al. 2004). Activity Theory is a constructivist theoretical framework that strives to understand the relationship between consciousness and activity, similar to Phenomenology (Nardi 1995). In the realm of HCI, Activity Theory is of primary influence through its emphasis on the

role that artifacts, like computers, play in mediating experience. It is through the artifact that humans engage and interact with external artifacts and other humans. At a basic level an artifact is language and gestures, but at a concrete level an artifact is a hammer and a keyboard.

Activities have a particular familiar structure, as seen in the figure below. For an individual, the activity is a set of actions towards an object to create an outcome. It is the object of an activity that distinguishes it from other activities; the same actors and artifacts may be used but with different objectives. For example, a director and the HIPAA explanation form may be used for the objective of notifying patients of their rights, but also for demonstrating to a licensing agent HIPAA compliance. An object can be something tangible, like a completing a form, or it can be a common idea (sometimes called an objective). The only qualification of an object is that can be used by the actor for manipulation. The relationship between the actor and the object is mediated by the tool, and the tool embodies that historical context of that relationship. As Kuutti explains, “The tool is at the same time both enabling and limiting: it empowers the subject in the transformation process with the historically collected experience and skill “crystallized” to it, but it also restricts the interaction to be from a perspective of that particular tool or instrument” (Kuutti 1995, p.27). The relationship between the subject and object is represented in Figure 10 in a red line. The mediation between the subject and object is represented in the black lines connecting them. The transformation process of actualizing the object into an outcome is represented in the arrow.

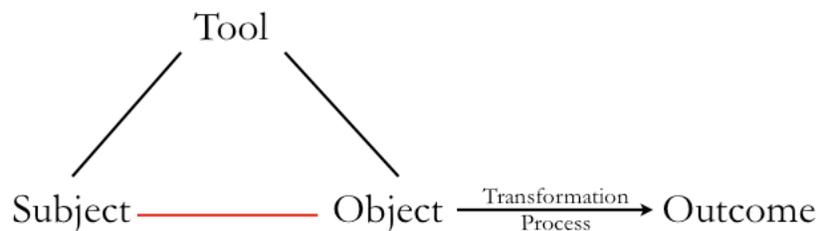


Figure 10. The form of an activity at the individual level, sometimes called Mediation Model (Mwanza 2001).

Figure 3, however, only captures the individual’s conception of the activity. The full conception of an activity involves considering the actor in her environment. Part of the environment involves the community that the actor is a part of. For example, a director is one actor in a community of administrative staff and additionally one actor in an even larger community of medical personnel. Communities are defined by sharing the same object. This is depicted in Figure 11 with the red lines between community-subject and community-object. (Figure 11 presents a simplistic view of activity. There are actually mediating relationships between all parts of the activity.) Considering the individual as part of the community is a foundational part of Engström’s contribution to the further development of Activity Theory (Engström 1987).

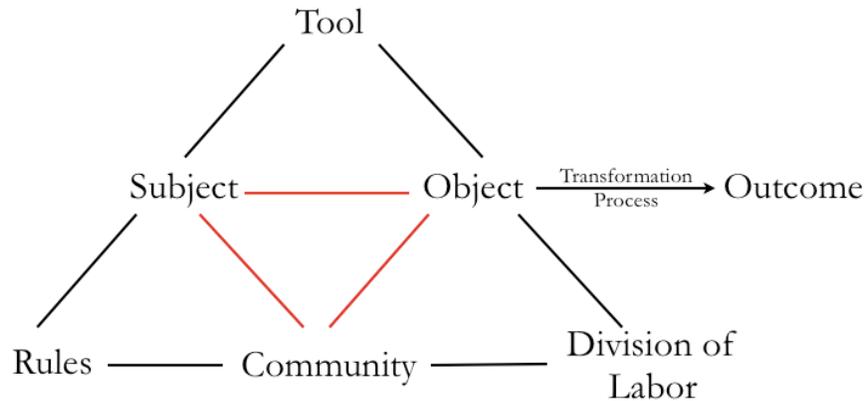


Figure 11. An Activity from the community and individual perspective, sometimes called the Activity Triangle Model (Engeström 1987; Mwanza 2001).

The relationship between the community and the subject is mediated by rules. These rules are the focus of my dissertation study. Rules may be explicit or implicit, as long as they are norms that regulate the activity. An explicit rule may be something that has been crystallized, for example, into a policy book that parents sign. An implicit rule may be something that every one understands but does not discuss, for example, a social norm in the settings that were studied indicated that other workers do not touch the medical director’s computer even though the computer is in a commonly shared space.

The relationship between the community and the object is division of labor. Division of labor refers to explicit and implicit organization of the community. For example, it is the job of the director to manage the patient’s files for the next day. Whereas it may be the administrative assistants job to print out the schedule for the next day and to check that it does not have patient information on it.

Given my focus on breakdowns in the current explicit and implicit policies being used in medical and childcare practices, there is a need to understand the theoretical underpinnings of how communities handle them. The ability for Activity Theory to be able to describe and provide a framework for labeling a breakdown is one of its strongest abilities as a theory to help answer the first research question. Activity Theory has a model of breakdowns that stem from Marxist Theory (Nardi 1998). When an activity system has a perturbation, it indicates that there is a need for growth; the activity system needs to change. A “contradiction” within and between elements of an activity, or even between levels of an activity, can cause a breakdown (Kuutti 1995). The cycle of a breakdown is that a perturbation is caused by a conflict or a tension within the system. A definition of breakdown is provided below:

**Breakdown:** When a perturbation occurs in the social system that causes a contradiction to occur between activities or within parts of the activity system.

Bardram provides an example of a breakdown from the medical field between the objective of the nurse and the doctor. In the example the nurse is trying to help the patient get out of bed (Bardram 2009b). However, what she does not know is that the doctor had

prescribed intravenous medication that requires the patient to stay in bed. The lack of coordination between the objective of the nurse and the objective of the doctor created a situation where two objectives became in conflict. Bardram explains that there are many times when the overall objective of the activity (i.e., healing the patient) becomes lost or drifts from the related individual activities.

The process of responding to the breakdown has been explained further by splitting the process into phases (Raeithel 1996; Nardi 1998; Nardi 2007). The activity system goes through phases where the system works and does not need change. This phase is called coordination. From coordination the activity system can move into a phase where there are minor disruptions to the system. This phase is called cooperation. Last, the activity system can move from cooperation into a phase where major breakdowns have occurred that require the system to realign, called co-construction.

Co-construction has been further explained by Nardi as when the collective group, or organization, needs to redefine their object(ive): “Co-construction necessarily involves intensive learning as new practices are being devised, which itself requires learning, and the new practices are intended to be learned by others” (Nardi 2007). The groups adapt to the new object through learning on a personal and community level. The group does this through object construction and object instantiation. Object construction is the process of figuring out what the object should be, of defining it, and motivating the activity (i.e., the process of figuring out how to get all the forms updated on time). Object instantiation is the work that goes into materializing the object, of incorporating the object into the activity (i.e., creating new forms or sending out emails). Through both of these processes the communities work to create change in response to a conflict or breakdown in the activity system. Using this framework affords teasing apart not only that a breakdown has occurred, but how the communities responded and instantiated a change.

In her work of using video data to examine focus shifts and breakdowns in using computer applications, Bødker suggests to ask the following questions that can be useful for identifying the cause of the breakdown in an Activity Theory framework (Bødker 1996): (1) For an individual, what is the purpose of the activity and actions? (2) When there is more than one person participating in the activity, are the tools, purposes, and objects conflicting between the individuals and groups?

### 3.3.2.2 Defining & Isolating Breakdowns

For this dissertation breakdowns have been used as an analytical framework for understanding where the current socio-technical system does not support the actors engaging in the activity of managing sensitive client information. Breakdowns, as discussed in the previous sub-section were encountered due to conflicting object(ives); conflicting rules and division of labor; uninstantiated rules, tool, and object; and inadequate object and tool. Each breakdown described in Chapter 4 lists the type of breakdown that was encountered and explains the circumstances. For each breakdown the actor is engaged in an activity that may be in conflict with another actor’s activity, or a needed tool or object is not present to guide that activity, or there were activities where uninstantiated rules caused breakdowns to occur.

The particular breakdowns that were isolated were ones in reference to privacy and security. Privacy is a contextual, individual, and negotiated construct. Therefore what is related to privacy and security for one individual, in one center, in one room, with certain people present, at a particular time is different from what another individual might consider. Additionally, what might be considered as a privacy or security breakdown by one might not be considered a privacy or security breakdown by another individual. The subjective nature of privacy and security, therefore makes them difficult to study when trying to present an objective understanding of privacy and security.

However, by asking people what they consider to be breakdowns or around topics sensitive to privacy and security phenomenon, what breakdowns are presented are representative of breakdowns. To determine what was related to privacy and security was determined by the participants. As the participants acted and interacted their reactions to interactions were noted. In instances where participants noted that their interactions were incongruent with client privacy, these were isolated as breakdowns. Similarly, when there were differences in opinions (e.g., between parents and childcare center directors), these were also noted as breakdowns.

In using Activity Theory I examined contradictions in activities, either through conflicting objectives or through uninstantiated rules or divisions of labor. For each breakdown I highlighted the part of the text that described the breakdown. I then memored each breakdown to explain in reference to Activity Theory where the breakdown occurred in the situation as explained either in the interview transcript or observation notes. I also included relevant artifacts in these memos.

### 3.3.2.3 Combining Breakdowns

After all breakdowns had been isolated, it became apparent that some breakdowns were relatively isomorphic; the breakdown had occurred because of similar conflicts. These breakdowns were collated. For example, many parents stated that they did not know who could access their child's information. All of these breakdowns were collated to one breakdown group. In total, there were 84 breakdown types divided by Study 1 and Study 2.

### 3.3.3 Phenomenology as a Response to Research Question 2

Because information systems in the large are not just technical but also social, the scope of privacy and security concerns must include social and technical factors. Clearly, computer security is enhanced by developments in the technical arena where researchers are building ever more secure and robust systems to guard the privacy and confidentiality of information. However, when the definition of security is broadened to encompass both human and technical mechanisms, how security is managed by the day-to-day social work practices becomes increasingly important. While research has argued that "users are not the enemy" (Adams et al. 1999), designers need acknowledge the social the social but in understanding and evaluating how social practice can be accounted for in models, like threat models, that are used in security analyses. However, accounting for social actions

in technical models is difficult because it involves studying the subtle and complex phenomena that surround people and their work practices.

It is for these reasons that there exists a need to evaluate what the phenomenon of security and privacy are within these settings. It is through valuing how privacy and security are embodied and lived in these environments that a greater understanding of how to design for them can emerge. Given the need to evaluate security and privacy as lived experiences, the qualitative inquiry method of phenomenology was selected as a research method to analyze the body of data. Phenomenology is study of shared experiences that is used by reducing the data from qualitative inquiry to a set of shared themes and meanings (Creswell 2007). In this section I present a short description of Phenomenology along with an outline of how it can be used for analysis.

### 3.3.3.1 Phenomenology as a Method

Phenomenology is a method of evaluating the meaning that is described by several individuals about the same experience (Cresswell 2007). Instead of focusing on a particular micro-culture, as with case studies or with ethnography, Phenomenology provides a methodological lens for examining a common experience of a phenomenon shared by a diverse group of people. The goal of this method is to reduce all of the shared experiences into the essence of phenomenon. This essence can then be described by conveying the “what” of the experience and the “how” it was experienced.

While the use of Phenomenology is not as pervasive within the human-computer interaction community as other methods such as ethnography or grounded theory, it has been used before in relevant literature. Perhaps the most cited example within human-computer interaction is Heidegger’s example of the hammer that goes from ready-at-hand to present-at-hand (Heidegger 2008). Heidegger explains how the experience of using the hammer changes while different affordances of its form take presence in the user’s mind. Heidegger’s foundational theoretical work has been used to explore problems of embodiment (Dourish 2004) and affordances (Carroll 1991; Turner 2005) that have had a cascading effect on the design community of human-computer interaction. Beyond this seminal example there have been more recent uses of Phenomenology in human-computer interaction. These include examples such as the experience of halting webpages (Rosenberger 2007), the experience of receiving phone calls (Light 2008), and the experience of the interaction between body and technology during play (Karoff et al. 2009).

In comparison to human-computer interaction, Phenomenology has been used frequently within the medical community (Cresswell 2007). The use of Phenomenology in this domain is perhaps a response to the anatomical and atomistic description of medicine instead of the human who is being cared for. For example, Phenomenology has been used to study the experience of having a disease (Baron 1985), of a near-death experience (Greyson et al. 1980), and of the doctor-patient relationship (Toombs 1987). By studying these phenomenon the focus can be taken away from the minutiae of the care and refocused on the overall experience.

As a method, Phenomenology has its roots in philosophy from the German mathematician Edmund Husserl in the early 20<sup>th</sup> century (Cresswell 2007). As originally conceived, Phenomenology was primarily concerned with consciousness, its structure, and the phenomenon that occur within it. Through the reflection on consciousness, and recognizing the relationship of the subjective and objective nature of interpreting reality, it was proposed that rigor could be used to understand the philosophy of knowledge. In reaction to the reductionist and objective approach to understanding the world, Phenomenology spread through Europe to develop into a qualitative method of inquiry.

Phenomenology, as with other methods, has seen a fair amount of debate as to different flavors and uses (e.g., hermeneutical, transcendental, psychological Phenomenology all have different views). However, there has been consensus about a few tenants of the method. The first is a concentration on the science of experience by the researcher through suspending judgment, or at least recognizing and attempting to document personal judgments (through bracketing and memoing). The second is that a user’s consciousness is directed towards an object, or “intentionality.” The perceived reality of the object is therefore inextricably entwined with how it is represented in consciousness. The third is a rejection of subject-object dichotomy due to personal meaning ascribed to any experience or object. The last is the emphasis on the diversity of experiences as reflecting different facets of a phenomenon. Together these tenants reflect an emphasis on understanding the objective and subjective reality of an experience and then distilling multiple people’s experience into the essence of a phenomenon.

With these tenants in mind, the method for conducting phenomenological research as explained by Creswell (2007) is presented. The first step involves determining the phenomenon to be studied. In my case, the phenomenon are privacy and security as the lived experience of managing a client’s sensitive personal information. The second stage is to collect data from participants who have experience with the phenomenon. The data is usually in the form of interviews, but can also involve collecting artifacts, using journals, or conducting observations. For this dissertation I conducted interviews and observations along with collected artifacts and created diagrams. In this method the research scientist then conducts data analysis on body of data using the stages presented in Figure 12: data managing, reading and memoing, describing, classifying, interpreting, and representing.

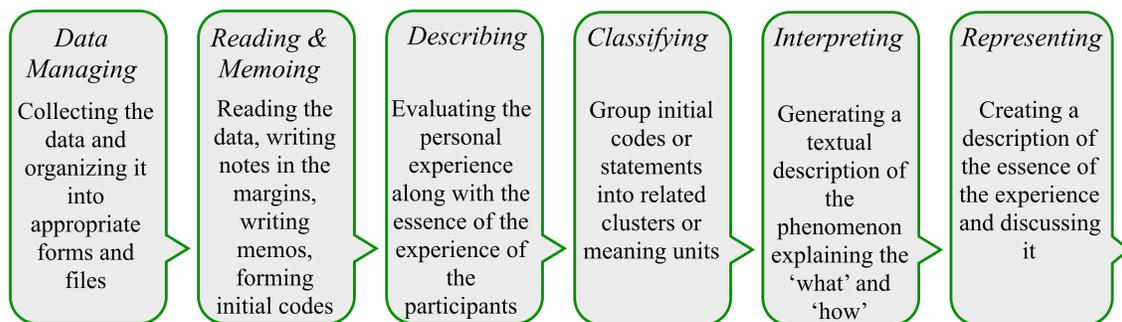


Figure 12. The phases of analysis when conducting phenomenological qualitative inquiry.

As with all qualitative methods of inquiry, the movement from one stage to the next is not necessarily linear (Creswell 2007). There are times when the researcher may move backwards or forwards a step as understanding emerges. However, there is a general path in the collection and analysis of data using Phenomenology. The first stage is documenting and continuing to document the researchers experience with the phenomenon (presented in Section 3.1.1.1). This allows the researcher to acknowledge his or her own experience in relation to those that are studied. The researcher then collects the data and the files are organized. The researcher next parses the data to find statements about the participant's experience with the topic, to create a list of the experiences. This process is called horizontalization. In trying to understand the participant's experiences the researcher can memo the data including his or her own perspective in brackets within the text. This list of experienced topics is non-repetitive and non-overlapping, meaning that each statement is considered as a unique perspective. These statements are then grouped, and the researcher provides her perspective on the experiences (presented as Appendix A). The researcher then describes how the experience was lived to create the essence of the experience

For my research, I progressed through to the stage of classifying for each of my data sets only to realize that I had not captured the essence of the experience. This caused me to iterate through the stages of data managing, reading and memoing, describing, and classifying five times before I started interpreting the data. The data collection and memoing process has been described in previous sections within this chapter.

The research presented in this dissertation has roughly followed the phases presented in Figure 12. All data was transcribed and organized into the data set. These files were then analyzed and read by at least two people. More data was then collected for the second study and added to the corpus of data. All data was then re-read and memo'd. Researchers then filtered the data down to the breakdowns that involve privacy and security and created a description of each using Activity Theory to isolate breakdowns and then Phenomenology to detail the relevant details for each lived breakdown. These breakdowns were then aggregated into themes to better explain the types of phenomenon relevant to the study.

### 3.3.3.2 Application of Phenomenology and Resulting Themes

The purpose of this work is not to demonstrate that n number of people observed the same phenomenon that were encountered by the researchers. In other methods, such as grounded theory or content analysis, rigor is demonstrated in the quantifiably objective reality that other researchers have seen (e.g., XX% of the breakdowns were labeled as breakdowns by n researchers). However, Phenomenology is not as concerned with demonstrating this kind of rigor in the data. The depth of analysis into the phenomenon, as explained by van Manen in his book on lived experiences, demonstrates rigor (van Manen 1990). The deep work of one could be more rigorous than the work of ten, depending on the analysis that is presented. This face is shown in the famous work of Heidegger (Heidegger 2008) and the more tangible work of Rosenberger on the phenomenon of slowly-loading webpages (Rosenberger 2007). Therefore, certain precautions as explained in this section have been taken to account for rigor in the data

collection and analysis: (1) all data was reviewed by at least one other researcher; (2) preliminary themes were all constructed and created with at least one researcher; and, (3) numerous collaborative discussions were held to analyze the phenomenon in question and to develop deeper insights.

The first three steps of the phenomenological method are described in Sections 3.2.1, and 3.2.5, and 3.2.7 on data management, reading and memoing, and describing the data. In regards to diverse array of data forms (e.g., interview transcripts, artifacts, observation records), the data was combined by first isolating a breakdown and then collecting relevant quotations from written records and pictures of artifacts into memos as a form of horizontalization. Data was read and re-read many times and discussed with other researchers to debate the inclusion of data into the isolation and boundaries of a single breakdown and then a breakdown type.

The data was then classified in two steps, which is described in Section 3.3.1.2 and 3.3.1.3. All data from Study 1 and Study 2 was included in this classification. The first step involved organizing the data into groups around the same type of breakdown. An example is “Disregarding Privacy Policy” in which participants were observed to be violating a policy surrounding how client information should be managed. The list of all breakdowns is included in Appendix A. Each breakdown was then described through memos in reference to security and privacy, which is also included in the appendix. This work resulted in 83 breakdown types divided by Study 1 and Study 2, some of which were related to the themes found in Study 1.

The second step of classifying involved the creation of themes. To create the themes, or as labeled in Figure 13 codes, two researchers met over a series of meetings to create and describe 16 themes that outline the types of breakdowns that were discussed and observed. Themes are broad categories that describe a particular phenomenon, or “clusters of meanings” (Creswell 2007, p.55). These themes were created by examining what had caused the breakdowns of that type to occur. The first step was reading all of the descriptions of the category and related examples. Once these were discussed the causes of the breakdowns were discussed. Groups of breakdown categories were then combined together by similar causes. For instance, all breakdowns that were caused by policy violations were grouped together.

Once there were representative examples of each theme, descriptive memos were created to interpret the overarching phenomenon being discussed including discussing the “what” and “how.” An abstract of each theme is included in Table 11. Once these memos were created the data was re-evaluated with a third researcher who verified the classifying of the data.

The last step was representing the data. This representation is presented as Chapters 4 and 5.

Table 11. Breakdown themes used to describe the breakdowns relating to security and privacy.

<b>Breakdown Themes Title</b>	<b>Description of Breakdown Themes</b>
Policy Violation	When there is an explicit policy governing how sensitive personal information should be managed, but the policy is not followed.
Access Policy Work-arounds	When there is an explicit policy governing how sensitive personal information should be managed, but the office staff find a method to get around the policy or a loophole.
Beliefs About Security	Ideas that people have about security and privacy that are questionably correct.
Human-Technology Mismatch	When technology exists that offers a solution, but the people do not like using the technology thus resulting in a situation that is less secure.
Inadequate Representation in Available Information System	A system exists that has all of the information that is desired, but because of the way the system is set up the user is incapable of using it. This is relevant for issues like access logs.
Information Acquisition	The centers having difficulty acquiring information that is sensitive.
Information System Problems	The information system exists but results in additional problems relating to managing client information (e.g., system crashing).
Information Withheld/Hidden	Information is sought, and the information exists, but a person enforces a policy restricting access to that information.
Local Negotiation of Content	The content that actually goes into the client's files is negotiated.
Local Negotiation of Policy	There is an explicit policy that regulates how the situation is supposed to unfold, but locally in practice the policy is different.
Access Policy	There exists a policy that is restricts access to some needed piece of information.
Practice/Performance Problems	In the action of enacting a policy there are difficulties.
Sensitive Information Publically Available	Sensitive information is viewable to anyone who walks by.
Social Relations Problems	Problems that occur socially that then affect client care or the management of client information.
Synchronizing Information with Reality	The information that exists in a client file is not representative of some objective reality.

### 3.3.3.3 Alternate Choices for Methodology

The questions are qualitative in nature. I seek to understand the shared experience of managing sensitive personal information. This cannot be studied using quantitative methods because statistical significance is not of value. Instead, what is of value is examining the multitude of complex voices and what they have to say about a phenomenon. This kind of analysis can only be evaluated using qualitative inquiry. Creswell explains that qualitative research “beings with assumptions, a worldview, the possible use of a theoretical lens, and the study of research problems inquiring into the meaning individuals or groups ascribe to a social or human problem” (2007, p.37). Through qualitative inquiry, a researcher can develop theories that then can be used to help expand on a problem, which could then be used to develop quantitative studies.

The “theoretical lens” used for my study is Phenomenology. Alternate choices are case studies, grounded theory, content analysis, and narrative analysis, and ethnography. In reference to security and privacy, they have been studied before using grounded theory (Mazurek et al. 2010) and ethnography (Adams et al. 2005b). These methods are useful for illustrating how culture affects security and privacy in reference to grounded theory, but are not correct for the research questions presented in this dissertation. In particular, grounded theory seeks to provide or generate some theory. The theory can be about how a system works or how a framework explains the issue being studied. My work does not desire to create a framework or workflow about how privacy is accounted for. Instead, it seeks to understand what the phenomenon of security and privacy are, without a focus on generating theory. Ethnography, particularly multi-sited ethnography, is similar to the approach presented in this dissertation. Ethnography, though, focuses on the culture of a particular group of people. The locus of study is on a particular place, with particular actions that need to be studied. This kind of study has a high degree of depth, and is divergent from my goal of studying the experience across numerous people, sites, and locations. Last, case studies are valuable for answering questions about a particular culture and then comparing cultures. My goal is not to compare across culture, but to do a holistic analysis of a phenomenon. This is not to say that differences do not exist, but studying differences is not the purpose of this study. It is for these reasons that Phenomenology is most suited for the study presented in this document.

### 3.3.4 Near-Future Scenarios as a Response to Research Question 3

The use of scenarios was selected as a method of explicating the underlying tensions, including the explicit and implicit rules, that guide the design space for security and privacy. Scenarios have a rich history of understanding the design space, and have been used extensively in the work of McCrickard and Chewar (Chewar et al. 2004; Chewar 2005; McCrickard et al. 2006). Particularly within this work they present the use of spectrums to understand and evaluate the central problems relevant for a set of scenarios. I have adopted this method for responding to Research Question 3.

To generate the scenarios the breakdown categories were considered along with the findings from the phenomenological analysis. Together a set of comprehensive scenarios was created. These scenarios were then paired to demonstrate the different aspects of the

design space, iterated on, and a final set of scenarios was created. These are presented in Chapter 6.

### **3.4 Summary**

The data in this study was collected in rural-serving southwest Virginia in childcare centers and physicians' offices from 2009–2010. Rural-serving southwest Virginia has valuable descriptive characteristics, including the ratio of uninsured patients (1/5), along with the digital divide that influences the adoption of electronic systems into these centers (Premkumar et al. 1999; Fruhling et al. 2006; Coburn et al. 2007; 2008). For instance, one of the physicians in this study explained to an observer that he was hesitant to take a tablet machine into the room with a patient because he felt that it might affect their interaction. Additionally, the surrounding universities influenced this area. This last characteristic made participant recruitment problematic, but also influenced the technology systems used in the centers.

In total 12 childcare centers directors participated in interviews and 14 physician's office directors. Four childcare centers went on to do observations. Only 2 physicians' offices allowed for observations, with an additional 3 centers recruited. Additionally 21 parents were interviewed. On average, parents had between 1 and 2 children and spent approximately 14 months in numerous childcares. Within the centers studied the directors had a large amount of experience with the average being 12 years for childcare center directors and 20 years for physicians' office directors.

Directors were the primary focus of interviews and observations. Directors had the most knowledge of interactions at the centers and had knowledge of who accessed what information. Additionally, client files tended to be co-located with the directors workspace. With these characteristics in mind, 126 hours of observation were conducted, evenly split between the two location types.

The analysis consisted of four steps, the first of which was collecting and transcribing all data. Activity Theory was then used to parse the data to a list of breakdowns. Phenomenology was then used to understand the breakdowns and how security and privacy were experienced in these instances. Last, a set of scenarios was developed in response to the breakdowns in a set of eight spectrums. The analysis is presented in the remaining part of the dissertation.

## **4 Privacy & Security Related Breakdowns**

In this chapter I present a list of relevant breakdowns based on the themes discussed in Chapter 5. Not all breakdowns are presented in this chapter, only the ones that are relevant. All breakdowns can be found in Appendix A.

In the previous chapter I defined a breakdown as a perturbation in the activity system that could represent a conflict between activities (e.g., protecting client information v. care of the client), between parts of the activity system (e.g., conflict between division of labor and rules), or when parts of the activity system have not been previously instantiated (e.g., how to manage rules with new tools).

All the breakdowns in this dissertation convey the story of what privacy and security mean in intimate, local, and negotiated work. In this vein, breakdowns from Study 1 and Study 2, breakdowns from interviews and observations, and breakdowns from childcare centers and physicians' offices have been combined to represent the rich body of data. Copies of all interview transcripts and observation notes with descriptions are provided in the appendix.

From the analysis of the data from Study 1 and Study 2's there were two hundred and eighty-one observed breakdowns, one hundred and fifty-five from Study 1 and one hundred and twenty-six from Study 2. One hundred and twenty-nine breakdowns were observed and one hundred and fifty-one were elicited from interviews. Broken down by location and participant there were one hundred and sixty-six from physicians' offices, eighty-three from childcare centers, and thirty-one from interviews with parents.

This chapter is presented as a summary of the data. Each section represents a theme presented in Section 3.3.2. Each theme is then discussed with example breakdowns. For example, in the theme of "Policy Violations," all breakdowns related to sharing logins are presented as an example of policy violations.

I present these results not to point at any one place where security and privacy were not accounted for. Instead, I present these results to provide interlaced examples to construct a broader understanding of security and privacy in the collaborative management of client information.

### ***4.1 Policy Violations***

Policies explicitly define the rules for how people in the centers should manage sensitive information. When a person does not follow a policy, such as when they access client information that they should not, or shout out client information across a shared social space, a policy breakdown occurs.

This section presents eight kinds of breakdowns where an explicit policy surrounding how a client's information should be managed was not respected.

### **4.1.1 HIPAA Violations**

There were four breakdowns where personnel in a physician's office raised the problem that the practice was not HIPAA compliant.

HIPAA, as discussed in Section 3.2.3, is a national standard enforced by the Office of Civil Rights to protect identifiable information about patients. The people who work in physicians' offices are mandated to keep client information secure through various procedures and security mechanisms. HIPAA played a large part in how participants managed patient information. It influenced the location of their filing cabinets, the printing and posting of schedules, the location of where certain information could be stored, and even affected their screen savers.

However, local practice and nuanced situations created tensions in following HIPAA guidelines. In the first breakdown, a nurse lamented to another nurse about how the physical location of the patient's files, which are stacked above the filing cabinets and not stored in a locked location, are not HIPAA compliant. When the nurse mentioned this problem to the doctors and director she found that they would not rectify the situation.

In the second example, there is a discussion between staff members about what constitutes as identifying information. In this breakdown an office staff member wrote down, left out, and shouted into the patient waiting room a patient's full name.

In the third example, a man called the office to try and locate his wife. The director provided the location of the wife, and afterwards a nurse instructed the director that this was a HIPAA violation. In response, the doctor called the nurse, "Little Miss HIPAA."

In the fourth example, an office staff member discussed how to manage the need for printing a medical record without a medical release. She explains that she knows that this is a HIPAA violation, yet believes the situation may require printing the record without the consent.

### **4.1.2 Doctors Exchanging Client Information**

There was one instance where a director discussed the need to share patient information without explicit consent from the patient.

Patient consent is required by HIPAA and also is a privacy mechanism for patients to protect their own information. As explained in the quotation below, there are time when the doctor has a need to do a quick consultation so that he can proceed with his surgery:

I often will call another doctor and say you know, I've got a patient here for surgery and he told me he had chest pain the other day. So they'll get a consult. Or if we get a pre-op EKG that looks a little funny to us, we'll often fax it to the cardiologist across the street. We'll often fax it over there and/or we'll call and say we have a patient with a question, will you look at the EKG.

This quotation illustrates when there are times when the need to acquire information that is critical to the activity is in conflict with the activity of protecting the patient's privacy. Specifically, the doctor needed the information about the client to proceed with his surgery, yet he did not acquire client consent before sharing the client's information.

### **4.1.3 Knowing Patients Personally**

There was one breakdown that was observed where a nurse called a patient immediately after receiving the results of her test at the office. The office that the nurse belonged to particularly took pride in knowing their patients on a first name basis, and being friendly with all the patients and patient's care givers who came in. They generally jested with the patients and made jokes.

This breakdown, though, went further than being friendly. The nurse explained to me that she knew the patient because she had helped them during an important medical crisis during her training to be an emergency response nurse. Given this intimacy, she acted against the policy of the center. This policy stipulated that the doctor calls the patient with test result. This nurse was not observed to be placing similar calls to any other patient when their test results were received.

What is important is that when the nurse obtains the patient's test results the privacy norms and rules surrounding appropriate disclosure become obscured. Is the nurse a friend with special information, or is she a nurse breaking a privacy policy? The ambiguity surrounding her role influenced how she responded thus resulting in a breakdown.

### **4.1.4 Staff Accessing Client Information that they Should Not Access**

In the interviews with childcare center directors they explained that the director works as a gatekeeper for the child's file. If anyone in the center wants access to the file, they have to ask for permission before looking at the information. The director for Child-P01 explained:

When a teacher comes in and wants access to a file they have to come through me first and they have to tell me their reason basically, you know, why do you need to go in there? Oh I'm looking up their middle name, oh I'm looking up to see what nationality they are, you know, so that I have an idea why they need to go in that file to make sure it's not being misused information.

When the director functions as a gatekeeper she is the enforcer of security policies about access.

Another important fact about Child-P01 and Child-P04 is that they are National Association for the Education of Young Children (NAEYC) accredited institutions. This means they have to have parents fill out a form saying who can and cannot access their child's information. A sample form is provided in Figure 13. This form is supposed to be

checked by the director before allowing anyone to access the information in the child's file.

**Consent Form**

Please read the following information carefully and initial in the box. Sign the bottom of the page.

**Infection Control Policy:**  
I have read the Rainbow Riders Infection Control Policy and understand that it is my responsibility to do my part to keep Rainbow Riders a healthy and safe environment for all children enrolled. I will abide by this policy.

**Permission to Post Allergies**  
I give Rainbow Riders permission to post my child's allergies in the classroom

**Release of Child's File Information**  
I authorize Rainbow Riders Childcare Center to release information regarding my child to the following agencies/individuals:

- Child's teachers
- Director and administrator
- Montgomery County Public School (if deemed necessary)
- Early Intervention of the New River Valley (if deemed necessary)

**Field Trips:**  
Field trips give us the opportunity to help children become more aware of the world around them. Throughout the year, field trips will be planned for different groups of children. Notes will be posted to give information about a particular field trip and for families to sign for permission. Field trips are a great way for parents to get involved and to spend time with their child. Please sign below giving us permission to take your child on field trips.

**Pictures:**  
Photographs are one of the many forms of documentation we use at Rainbow Riders. We use them to show a child's learning through the many activities of the day. Many of our teachers present workshops as a part of their professional growth and use pictures of the children to share information. Please sign below for permission to photograph your child and to use the photos only for professional purposes.

**I have read and consented to the above.**  
**Child's Name:** \_\_\_\_\_  
**Parent Signature:** \_\_\_\_\_  
**Date:** \_\_\_\_\_

Figure 13. NAYCE required form that asks parents to select who can access their child's information.

During an observation at Child-P01 a teacher came in and attempted to access the files for the children in her classroom. A snippet from the observation notes is included here:

A teacher appears in the doorway and walks into the room and approaches the corner of <the directors> desk.

"Hey," says the director.

The teacher says, "If I want my kids' middle names, are they gonna be in here or in the file?" <points to black box>

"they'd be in their file"

The teacher then says, in a much softer voice, "can I dig?" The informality of this word, the tone of her voice make this seem like a common practice.

<The director> responds with a carefully-laid sentence and a slight sternness in her voice, her eyebrows raised, eyes widened, and a scolding manner in the slow, undulating movements of her head and voice as she speaks: "I'll have to dig for you." I can only see the side of the teacher's face, but she looks shocked in that her face pauses, gaze held with <the director>'s, and there's a space created that seems to beg of a verbal response. <The director> fills the silence with a soft, earnest "I'm sorry" that seems to answer the teacher's unspoken question: "I can't, really?" It convinces me that this is usually not the situation the teacher finds herself in.

In this breakdown the policies of the director acting as gate keeper, and the extra policy of needing to check each file to see if a teacher can access the information, is put to the test. While the official policies were followed, the observer reflects that the behaviors demonstrate that this was not the typical circumstance. Indeed, later a teacher was observed to access the children's files without the director's supervision at the same childcare center.

#### **4.1.5 Client's Family, Friend, and Neighbors Discussing Client Information**

There were four breakdowns where someone external attempted to access client information.

In the interviews with childcare center directors and physician's office directors a table was provided to them asking who could access and how access was granted to client information. One set of stakeholders both types of participants were asked were family members or friends. All childcare center directors reported that, without permission from the parents, no one could access the child's file. Similarly, all but two physician's office directors reported the same thing.

However, there were times when external people wanted access to client information. In one breakdown a director explained that sometimes grandmothers call trying to pay for services. The director explained that unless the parents explicitly say that the grandmother cannot pay for services, they will accept payment from the grandparents. The second breakdown came from a director who explained how he receives calls from his patient's children asking questions about their parent's medical procedure. The doctor explained that he generates an "understanding" with these people, because "often" it is someone that he has had contact with previously.

Often those folks are old, and lots of time one of their children will call in and say you know my 86-year-old mother you gave an epidural to last week. And I always tell them to call in a week and let me know how they're doing. So it's often a daughter or a son or sometimes it's a next-door neighbor. But it's always someone who you've had contact with before so there's an understanding that they have access to that information.

Given the fact that external people contact him by phone, he has no ability to verify who the caller is before discussing client information. Additionally, even if the person on the phone is who they say they are, he does not verify that the patient has provided consent.

During observations there were two breakdowns where external people requested client information. The first breakdown occurred within a childcare center. In this breakdown a parent requested the phone number of another parent, and the phone number was provided without checking with the other parent first. The second breakdown is the same one discussed in Section 4.1.1 on HIPAA Violations. In this breakdown a husband called the center to try and determine the physical location of his wife, which is protected by national regulation.

These breakdowns occur because client privacy is not being protected in all cases, and in some cases the activity of providing and sharing a patient's care are not being properly managed. While the rules are clear (e.g., do not share a client's private information with external people), this activity is not necessarily congruent with the activity of managing a patient's care.

#### **4.1.6 Sharing Login**

There are three breakdowns where individual passwords are available, but they were shared in one childcare center and two physicians' offices.

Sharing passwords means that one person would be logged into a machine, but people in the office would share that machine instead of logging the prior person off and logging in with their account. This represents a security problem because there is an inability to audit who changed and accessed client information.

In the first breakdown from a physician's office, the "Medicare Queen" of the office needed to log into the hospital's electronic database to collect information about a newborn infant. However, she has not attended the course and received her own individual access. To get this information she asked the person who does have access to log her in.

In the second example, the director explained that at the start of a day the staff log into their computers and use that login all day. As people move throughout the office they will use another's machine because everyone in the office "has the same access" and "there is no real privacy act between employees." Because everyone has the same permission, there is no need to have an explicit rule specifying that they can or cannot use each

other's computer. This fact is inherent in the work that they do and the information that they are all allowed to see, access, or modify.

In Child-P03, there is only one password that everyone shares to access the archives from the web-cameras. While the staff does use individual passwords for their electronic record system, the director reported that they do not use it for them for this system.

Similarly, at Child-P06 a teacher wanted to use the computer in the lobby of the childcare center. She asked the director, who is in the next room, "what is the password?" The director loudly shouted the password to the teacher.

#### **4.1.7 Disregarding Privacy Policy**

There were four breakdowns in relation to how patients interact with the privacy policy.

When patients first are seen at a physician's office they are provided a copy of the privacy policy that outlines what is a privacy breach and how the patient's information is managed. The patient must sign the form and return a copy to the receptionist. These policies are usually also framed on the wall in physicians' offices waiting rooms as shown in the pictures below. They outline the rights of the patient and how the records are managed, stored, destroyed, and who has access to them.

During the observations many new patients were observed, yet the patients spent little time reading and returning the form. No questions were asked of the receptionist, and no attorneys were called to check on their rights as patients. Similarly, the receptionists and nurses were not observed to be interrogating the patients about their privacy rights. While the last two cases are a bit of an exaggeration, patients and office staff were observed to not show concern over how client information was being managed.



Figure 14. Sample patient privacy polices displayed in the waiting rooms of physicians' offices.



Figure 15. Sample patient privacy policy displayed in the waiting room of a physician's office explaining how records are retained and destroyed.

In specific examples, patients were observed at Med-P15 and at Med-P16 to say that they did not “care” about the privacy policy and that they were not going to read it. In neither breakdown did the office staff tell the patient that not looking at the privacy policy is against their best interest. In fact, a nurse at Med-P16 said that for all intents and purposes the patient can wall paper his bathroom with the policy.

Other breakdowns demonstrate difficulties in office staff using HIPAA and requiring patients to read the privacy policy. For example, in an interview with the director of Med-P18, the director explained that many of her patient’s “don’t want” the privacy policy. Also, that she “hates” HIPAA. T

he director at Med-P04 reflected the same sentiment as well. The director explained that while he understands the need for HIPAA, he believes that it is overly encroached how he wants to manage his patient's privacy. The example he provided in his interview is that he believes that it is common sense to not shout the patient's medical information in the waiting room. At the same time, though, he finds HIPAA overly restrictive.

Now HIPAA in my opinion, and I don't mind if this is recorded, I think it's a stupid thing. Now most of the stuff, with exception of the electronic transfer of information, the rest of it ought to fall under ethics not under law. Now I know there may be a fine line between there but I think it's an ethical dilemma. I wouldn't go out in the waiting room and say, you know, 'hey Ms. Jones your syphilis test is negative,' so to me it's an ethical thing and not a legal issue. Now maybe I'm not being fair. But they actually say, now my understanding of HIPAA interpretations, you're not even allowed to say the patient's name in the office. But what a load of crap, all that. I mean, when the patient comes in I'ma give her a hug, and love on her, and you know that's. If I got an 80-year-old lady, she wants a hug. I'm not gonna ignore her, you know, '205, you're up!' That's just, that's a little ridiculous.

These quotations and examples in regards to HIPAA reflect two sets of rules: the official policy of how patient information should be managed, and the local practices for how patient information is managed. These two practices appear to be in conflict.

#### **4.1.8 Lack of Password Use**

There were six breakdowns where participants were observed to not use passwords when accessing private information.

There were only two observations in all the studies that an individual log-in to any electronic system was observed. The first time was when two office staff shared passwords to get into the hospital record system. The second time was when the office staff logged out and logged back in between checking email (from observation notes of Med-P14: "... PR2 is still typing and clicking in MediaDent. She quickly checks her hotmail and re-launches MediaDent and logs into it with her user ID and password"). Instead, computers were used as communal tools, like a kiosk, that anyone could use for the work they needed to accomplish. Passwords were not used on these kiosk-like machines.

There were three breakdowns during observations where the observer noted that passwords were not be used. For example, the observer writes about Med-P16 while watching the director, "<the director> brings a paper over and punches it on the counter next to me. She leaves her office with it, leaving her computer unlocked." This example is conical of how office staff would (a) leave their computers open when they would leave their workstation, and (b) the general lack of concern about leaving a computer unsecure.

There were three breakdowns discussed in interviews about the lack of password usage. The most representative of these comes from the director of Med-P01, who reported that her office does not use passwords because “<people in the office> can access anything. That’s their job.” The office director sees having unlimited access to patient information as a requisite to the role of being an employee. Similarly, the director of Med-P07 explained that her system does not even provide multiple logins for each person, so there is no point to use them. Last, the director of Med-P19 explains that even though each person has their own unique login “they have the same password and they have the same access within the system.”

These breakdowns reflect the fact that even in places where passwords do exist, the need for this security tool is not represented in the work that people do. Or, to put this much more simply, because people in the centers do not see the need for passwords, they are not used.

## ***4.2 Beliefs About Security***

Security is not merely the enactment of policies. Security can be embodied into the beliefs that people have about it. Through these beliefs, people can behave in ways that reflect correct or incorrect security practices that were discussed in interviews and observed in action.

What is important about security beliefs is that without contradiction, they will persist due to their individual nature. Beliefs, even when contradicted, can be hard to change due to cognitive limitations such as confirmation bias and an escalation of commitment (Cialdini 2001). Because of these psychological issues, it is important to understand what security beliefs exist. The goal is not contradict them, but to identify how to design for and with them. For example, how do you design a security mechanism for people who believe that a computer virus can be contracted through a secure website? To explore this issue I present breakdowns in regards to security beliefs that influence the management of sensitive information.

### **4.2.1 Incorrect Beliefs About Technology**

There were three breakdowns where participants had incorrect beliefs about technology that directly influenced the security of client information.

An incorrect belief about technology is one where the person lacks knowledge of how a technical system works. In reference to security and privacy, these beliefs can be harmful for how client information is managed as illustrated in the examples below.

In the first breakdown, a Department of Social Services representative was conducting an impromptu inspection of a childcare center. As explained in section 3.3.2, DSS Representatives check the safety of the facility and the security of the information being stored there. While verifying the safety and security, the licensor may take notes or document information about children and a child’s file in her laptop.

During the observation the licenser expressed her beliefs about the use of passwords. She explains that no matter how good the password is, if someone wants access to the information on her computer they will be able to access the information.

So, we've got password protection. There's password protection for everything. They're like 'don't write it down', I'm like 'excuse me' <inaudible> ... if somebody really wants on they're gonna be smart enough to get on it, whether I have a nice long 12-letter multi-digit pass code or not.

While there is a small element of truth to her statement, the general statement is false. Her belief is that passwords, and security in general, are fairly useless. This uninformed belief is reflected in how she stores information on her machine, the passwords she chooses, and other critical decisions in the handling of sensitive personal information.

Other incorrect beliefs that were expressed by participants are the belief that by not having the URL for the web-camera system linked to the website for a childcare center, that it was more secure; and, that the use of Facebook caused the center's computer to fatally crash losing client information.

#### **4.2.2 Menacing Outsider**

This single breakdown represents the only time that a security threat was actively discussed during any observation. While the director of a childcare center was responding to email, she discussed with the observer a man who handles the lawn care for the surrounding buildings. This man happens to linger outside the front of the childcare center. While there was nothing particularly menacing about his behavior, she described how he talked to women who left the building as "creepy."

This breakdown represents conflicting objectives: the childcare center desires external people to remain far away from the childcare center in order to protect the children; the man presumably desires to talk to young attractive women who work at the center.

#### **4.2.3 Parents Lacking Confidence in Childcare Centers Keeping Information Safe**

Ten out of twenty-one parents responded that they lack confidence in how their childcare center managed their information.

Childcare centers have the double task of managing the care of the child while also managing the care of the child's information. However, the parents reflected that the people who were hired to work at the childcare center were probably hired more for their skills in caring for children rather than managing privacy. For example, one parent said:

I trust them. I do. I believe they collect and use the information in good faith; I don't presume that there would be a violation of confidentiality that was deliberate. My concerns are more around, you know, they're daycare workers not security officers. What they do they really know about

securing information? And, if it is information that is on the computer, they are not computer scientists.

The parents intrinsically value the care provided to their children. Yet they recognize that the center is not a facility with heightened security procedures around the management of the children's information.

Similar to the sentiment from the DSS inspector discussed in Section 4.2.1, parents additionally stated that they do not think that their child's information is insecure due to malice, but more due to inadequate knowledge. This is demonstrated in quotations from parents:

I don't think that they would willfully disseminate any information. I just, knowing people, and knowing that kind of stuff, I am not at all confident that someone couldn't break in or access that information illegally.

There are always those people who let things fall. She hands the office over to other people to work and a parent comes in and sees it on a desk. I believe when you are dealing with that many kids it is going to be kind of hard to uh keep everything locked down from all eyes.

I would say that uh I don't think that they going out and trying to sell my information to make money but I think that there would be an opportunity uh inadvertently for that information to get out. So you know I do trust them to not go out and do it maliciously.

Parents, in general, stated that they believe that there are procedures for managing information, but due to the hectic nature of the center that it is difficult for all information to be kept secure 100% of the time. This leads to parents lacking confidence in how their information is being managed.

When parents discussed this lack of confidence, they would make reference to relationships that they have. These relationships functioned as substantial building blocks for parents to trust the center's staff with the management of their child's information. For example, many parents cited their child's teacher as someone that is trustworthy.

Cited more frequently was the relationship between the parent and the childcare center director. Parents explained that they trusted the competency of the childcare center director. It was everyone in the center that the parents did not know who the parents believed were untrustworthy: "Not that you can fully trust anybody but I feel comfortable with the people that are in charge." These relationships served as the basis for parents to rely on the childcare center to manage the child's information.

However, there were examples where the parent did not trust their childcare. For example, one parent explains that she relies on her family, who lives within five minutes of her childcare center:

I trust them because out of my immediate family all of them are there with in five to ten minute drive from him. So, I don't necessarily trust (Vega) so much as I trust to be able to get in contact with my family and get them to help or get them to go get him or whatever the need be if I must be out here as it were.

#### **4.2.4 Parents Not Knowing Who Can Access Their Child's File**

Eleven out of twenty-one parents stated that that they were not sure who had access to their child's information in response to the question: "Who do you believe has access to your child's information?" What is important and relevant to this issue is that when discussing with childcare center directors about access policies, all childcare centers had clear rules surrounding who in the center could and could not access the children's information. These rules, though, had not been clearly communicated to parents as indicated with the data.

Over half of the interviewed parents reported that they were not sure who was accessing their child's information. For example, one parent responded, "No idea. Never thought about it." While this response was extreme, it reflects the lack of knowledge that parents had about who could access their child's information.

Many parents, after probing about whom they thought could and could not access their child's information, stated that they "assumed" various people accessed their child's information. Some parents stipulated that anyone could access the information with some parents only feeling comfortable with the directors and owners. This comfort level is reflected in the following quotations from parents:

I would say that I would feel feel comfortable with just the office manager and the owner there having access.

I am assuming...we have two owners and a director and assistant director. And the assistant director is also a teacher in one of the classrooms... I think these four people.

I assume the secretary and the manager, like the owner, manager-owner, I assume just that. Not even the teachers. Not the teachers.

I assume that any of their workers would have access to the records there.

This range of guesses and comfort levels demonstrate a lack of knowledge and ambiguity about how information access is actually managed and explained to parents.

### **4.3 Human-Technology Mismatch**

There were breakdowns where the user reflected that she wanted to interact with the technology in a certain way, but this interaction was unsupported. In essence, there was a

mismatch between what the technology would allow and what the user wanted to do. Some of these mismatches were related to security and privacy. The examples discussed in the sections below demonstrate two types of mismatches: the difficulties in using the system to locate patient files, and the auditing of other office staff's work.

#### **4.3.1 Difficulty Locating Client File**

There were sixteen breakdowns where participants were either observed to have difficulty locating client files or discussed difficulties in not being able to locate client files. These breakdowns were categorized as human-technology mismatch because the file presumably exists; yet, it is because of the participant's inability to use the system that a breakdowns occur. These breakdowns result in additional patient files being created, files not being in the correct location, and lost client information.

There were two breakdowns discussed in interviews with childcare center directors related to this topic. The directors discussed that they would "pull a file to look up somebody's phone number and the file won't get put back and then it gets buried on the desk." This misplacement resulted in problems locating the file when needed in the future.

The remaining breakdowns were derived from observations of three physicians' offices. Example causes for these problems were the unusual spellings of names, transposed names, and the office staff misspelling or misfiling. These problems are interrelated because the patient's name is the primary key for locating a patient's file. When a patient's file cannot be located based on the primary key, it is difficult if not impossible to find the file again.

An additional reason that physicians' offices had difficulty locating a file was due to office workflows. For example, one office had a separate location for when a patient's file needed a transcription, if the patient was going to be seen that day, if the patient's file had been audited by the doctor, if the patient had a particular medical device, if the patient was waiting for a return phone call, if the patient's file was going to go home with the doctor that evening, if the patient's file needed to be faxed, and then differentiated locations for how long it had been since the patient had last been seen (within the last year, within the last seven years, or longer than seven years). Due to the different actors conducting different activities, the file would be placed in different locations. For instance, one nurse needed a patient's file for the patient's up-coming visit, but the receptionist had the file in the pile waiting for a transcription.

#### **4.3.2 Inability to use Electronic System Results in Information Duplication**

Duplication of information was inherent in the offices that were observed. Patient files were duplicated across four files at one location: electronic and paper billing records, and electronic and paper health records. From a threat model perspective, duplications in the system mean that there is a higher chance of information leaks. Therefore, duplication can be seen as a hindrance to the security of client information.

During the observations there was one breakdown where duplication of information was related to human-technology mismatch. This breakdown related to the use of a “tickler file.” A tickler file is used by many businesses in order to “tickle” clients into returning to the business. In physicians’ offices they are used to ask patients to visit the office for regular care.

In the breakdown observed at Med-P16 the director had printed out her tickler file and was going through it from top to bottom. In between calls she explained that she could do the entire process through the computer, but the doctor does not like that method. The doctor believes that it does not provide enough over-sight. In a sense, the doctor wants to be able to audit her work, which he believes he can only do through the use of paper. This breakdown exemplifies how the doctor’s dislike of using the electronic system resulted in additional duplication.

#### ***4.4 Inadequate Representation in Available Information System***

The office staff populated the information systems with client information and meta-information (e.g., access logs, when information was entered, etc). However, there were breakdowns where the current representation of client information was deemed as inadequate by the patients or the staff. The lack of adequate representation led to providing additional information about the clients, information duplication, and dispersion of information.

##### **4.4.1 Client Providing Perceived Unnecessary Information**

There were five breakdowns of patients or parents providing extra information to the childcare center or physician’s office.

Extra information is information that was not requested by the center. Instead, it is information that was provided by the client without provocation. For example, one parent explained:

And in addition of that they did not prompt me for but I wanted to provide information on what he likes to do, how to comfort him, things that he enjoys doing. So, they did not have any specific forms for that but I wanted to make sure that they had the information and also the daily schedule.

This extra information facilitated a less “sterile” story of the child. Similarly, patients were observed to provide a page or half a page length description of all of their illnesses that was hard to convey on the forms.

What is important about these breakdowns is that the client is providing additional information that has to be managed, secured, and kept private. However, the centers regard this information as extraneous to the care of the client. An example from observation notes demonstrated how a parent came to a staff member with information about his new infant:

She doesn't know why he handed it to her, but he did. <The director> says that sometimes patients hand her information like this and she says it makes them feel better to give them a copy, even though she doesn't think that they use them.

These breakdowns represent conflicting objectives. The client desires to provide extra information, yet the centers regard the information as superfluous.

#### **4.4.2 Fields Not Providing Enough Patient Information**

There was one breakdown where the current electronic system required filling a field with a code to list information related to the patient's care. These codes are uniform across the system and are used to link standard procedures with client care that can help for billing and for sharing information with other physicians' offices. While observing Med-P16, both the doctor and the director explained their electronic system and how they associate codes with client care. What was unique about their practices is that the doctors do not feel that these fields provide adequate representations of the client's care.

For example, in one of the centers the doctor wrote letters and notes describing the procedures that captured the nuances that he believed to be important. The electronic system, in contrast, only facilitated storing the codes, which are also valuable. However, as the doctor and director explained, the codes do not capture the same information; they are not "accurate." For this reason, the doctor made additional annotations about the patients care that are not stored in the electronic file.

#### **4.4.3 Not Knowing Who Accessed or Modified Client Information**

There were five breakdowns discussed in interviews with physicians' office directors where the director discussed the lack of an audit trail.

An audit trail can be used to determine who had accessed and modified a patient's file. It provides the ability to determine what changes have been made, who made them, and when they were made. They can be useful for tracking errors, determining accountability, and following patient care.

As discussed in previous sections, participants in general did not use passwords. When passwords were used, they were shared. The lack of password usage and sharing passwords means that there is no ability to track who actually made any change to the system using the current security mechanisms.

The fact that audit trails are not used is also reflected in the open access and shared responsibility of client care. For example, only one director mentioned how she tried to manage the lack of an audit trail with the need to know who made changes in the file system. She explained that she has people write their initials when they make a change in the system. Because she is the only person who logs into the system, but not the only one to make changes, the initials allow her to review changes while still allowing open access to information. She explains:

Yeah because it doesn't show who's logged in and most of the time I'm logged in in the front because I'm the only one up there, but occasionally someone else will come up and they'll just do it, and I usually check to make sure just because it is on my login, but that's one thing is we wanted it to actually show who's logged in.

The problem is not the same in the management of physical files. This is because physical files afford more surveillance. For instance, if Jane is seen over with the files in the "B" section, and the file for "Baggins" is missing, the director knows to discuss the missing file with Jane. With electronic files, all access looks the same.

#### **4.5 Information Acquisition**

Information that is documented has numerous sources. One of these sources is the client. Both parents and patients provide information when they first enroll; when they talk to a director, teacher, nurse, or other office staff; and, when they fill in periodic forms throughout care. Gaining up-to-date information, though, was found to be a particular pain point. These problems are discussed in this section.

##### **4.5.1 Difficulties Gathering Information from Parents/Staying Up to Date on New Information**

There were nine breakdowns where childcare center directors reported difficulties acquiring new information from parents.

When a child is first enrolled the parents provide extensive amounts of information about their child in order to ensure enrollment. After the child has been enrolled, though, information about the child may change. The simplest example is that a child may receive immunizations. Gathering this new information is difficult for the childcare center because, as it is perceived from the childcare center personnel, the parents are too busy and they do not value returning new information. In the quotation below from the director of Child-P04, the director reflects that the sentiment of all of the childcare center directors:

They'll say 'I didn't know there was a parent meeting, and we put out an annual calendar just like this that captures August 6, 2009 through August 4, 2010. And, they'll still say 'I didn't know there was a potluck tonight.' And, we do, the classrooms do monthly newsletters, too, so they always capture important dates there. But they're still 'I just had no idea.' So, yeah, that does happen here. I know in the blue room, they tried to get photographs, they wanted family colleges, and I think they finally got up to about 50% participation. That was after, you know, a face-to-face transition meeting, they gave them the form, you know 'we just want to make a collage, we want to get some family pictures up,' a couple newsletters you know reminding them, and then at the parent meeting they reminded them. And, they were like 'we don't know what else to do, <Director>.' Well, just put up the ones we have. So, yeah, our parents are busy and juggling a lot...

There are many mechanisms that were utilized by directors to try and gather the new information. For instance, I was able to observe a director from Child-P04 for three hours while she was going through all of the children's files to see what information was not up-to-date. This director had problems that included forms that were completely empty, forms that were missing, pieces of information on a form that was missing (e.g., social security number, insurance ID number, secondary contact information), missing verification of a birth certificate, updated immunizations, and more. To gather this missing information she employed mechanisms such as texting parents, sending the parents emails, and also putting copies of the papers that need to be updated on the outside of the file for when parents come by. The diversity and breadth of what information could be missing in a particular file demonstrates the difficulties in maintaining a child's file.

Another mechanism used by childcare centers is the ambient information displayed in the environment to educate, communicate, and indicate when childcare centers need updated information from parents. Examples are shown in Figure 20. However, these displays may not be as effective as childcare centers would like. From the moment that parents enter the childcare center there are papers on the doors, papers taped to windows, bulletin boards, health inspection notices, flyers on washing your hands, lists of all the illnesses in the center, packets of information to be passed out to each parent, calendars, and dozens of other sources of information. With all of this information in the environment, it can be difficult for parents to attend to what is new and relevant. This has caused childcare centers to start to employ large "Read Me" signs, as shown in Figure 16.

In all of the observations of childcare centers, parents were never observed to read any of the information provided in the environment.

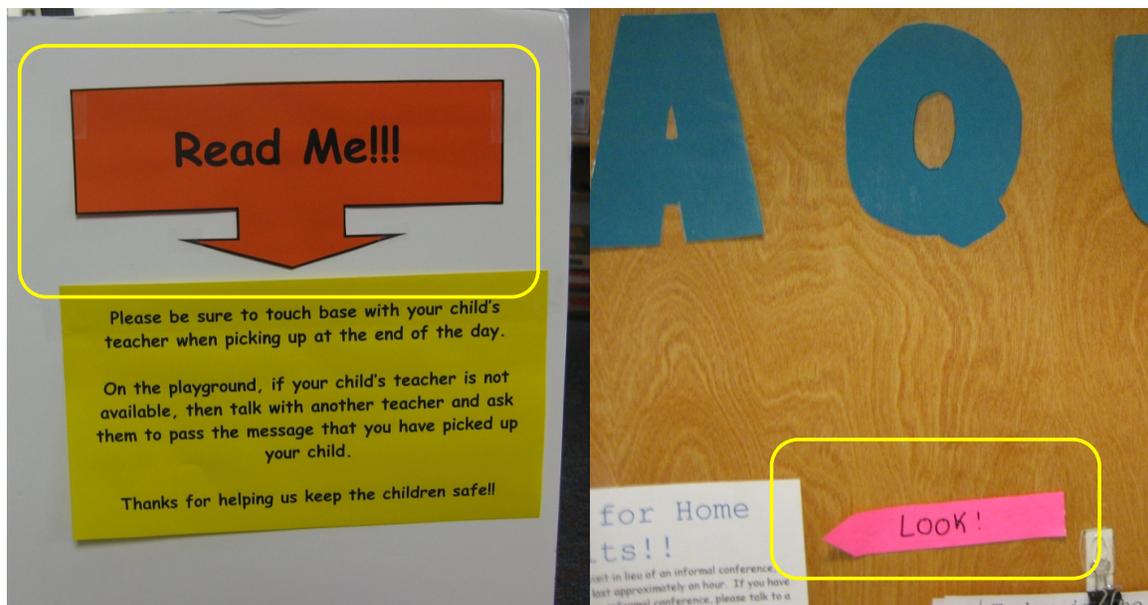


Figure 16. Example "Read Me" sign used in childcare centers to encourage parents to read the bulletin.

### **4.5.2 Patients Not Recognizing Updated Information**

There was only one observed breakdown of a physician's office where a director expressed concerns over acquiring information from patients. This is perhaps because patients have routine time with a doctor or nurse during their visit to the center. However, both Med-P16 and Med-P15 were observed to require non-routine patients (i.e., patients with non-weekly appointments) to fill out new paperwork about their medical history and information about their medical disorders. The director from Med-P16 explained that patients often think that they have provided up-to-date information, but when she compares the new information with the old, there is usually always something new.

### **4.5.3 When Staff Does Not Document "Adequately"**

There was one breakdown where a childcare center teacher was deemed to not be documenting an adequate amount of information about the children in her room.

Childcare centers have varying policies on documentation. While some policies regarding documentation are required by Virginia's Department of Social Services, most policies governing when something will and will not be documented are local. For instance, some childcare centers like Child-P04 and Child-P01 document weekly developmental milestones. Examples include activities such as stacking blocks or sharing with another child in a new way. These documents are then stored in books that the center shares.

Within Child-P01, there was a discussion during one of the administrative meetings about a teacher who was not working on her "Me Books." Me Books are books that are made for each child with pictures and stories of how the child is playing. Or, to use a phrase from the director, when the child is "working" ("To a child, playing is work"). The Me Book documents the work of children to make sure that they are progressing and to allow the parents and teachers to discuss issues related to the children. Given the number of children in each room, this documentation can be a large amount of work for the teacher.

The problem discussed in the meeting was that there was a teacher who was not working on her Me Books adequately. An office staff administrator reported that this teacher had not worked on her Me Books in seven months. The owner of the center concluded that the teacher should be "pulled" from the room. This means the teacher should no longer be a full time teacher in charge of tasks such as documentation.

## **4.6 Information System Problems**

Once information is within the system, either or electronic or paper, there are conflicting beliefs and issues related to the longevity of that information. The sections below present data that demonstrates that some patient files have indeterminate shelf lives, and other issues relevant to information system management. In general, this data indicates that paper information systems were easier to maintain, whereas electronic information systems required numerous back-ups, duplications, and security procedures that the office staff did not understand.

### **4.6.1 Client Information is Permanent**

There were sixteen breakdowns discussing the longevity of client information.

For all of the physicians' offices except for Med-P01, Med-P06, and Med-P16, who only kept their client's files for seven to ten years, all offices reported that they kept both their physical and electronic files indefinitely. One physician's office director reported, "No we even have the deceased; we don't get rid of anything." The oldest files in the study were from the 1930s, with a director who was the third generation doctor in his family ("We've got everything from 70 some or almost 80 years to 14 weeks"). As for childcare centers, there was a similar trend to keep certain children's files indefinitely.

Reasons provided for keeping the files for so long were because the electronic file system could crash; because the director reflected that the files represented his "life's work;" because the center was unsure what else to do with the files; because the center or doctor might be sued for mal practice; because the center wanted to support the community, e.g., to be able to identify the deceased ("The problem is, and someone wouldn't think about why it's so important, but it's like the Virginia Tech massacre we had 3 patients who we had to identify the bodies"); because the center's staff believed there to be a law stating that they needed to keep the files that long; because the director did not feel comfortable being the authority for deleting the files; and, because the system did not let anyone delete a file but only mark the patient as inactive ("We can make them inactive, but you can't delete them").

When a patient provides their information, it is unlikely that they consider that their information will permanently be stored. All of the parents in this study believed that after their children stopped attending the childcare center; their files were disposed. There was only one parent who could remember how long their childcare center stated how long they would keep their child's information. Parent-P12 reported that her childcare center would dispose of her child's file after six months of her child's departure. No other parent could remember any other date.

In general, it can be extrapolated from the data that clients assumed that after a reasonable amount of time their file is deleted. In essence, clients assume that their information has the same shelf life as their business. However, this assumption was found to be generally false for the centers in this study.

Medical files and child files are much more permanent, especially if the client is difficult or left the center under unusual circumstances. The director from Child-P03 talked about an incident where a teacher placed a piece of tape over a child's mouth. Not only is the teacher's information permanently kept on file, but the child's information is kept in case of a pending law suit.

#### **4.6.2 Electronic Record Systems Crashing & Loosing Client Information (and Fears)**

There were five breakdowns where the participants reported their electronic system crashed and lost client information.

The use of electronic system was abundant. All but one physician's office had some form of electronic records to manage their patient's care. All twelve of the childcare centers also had electronic system.

All participants were asked if their system had crashed at some point. Most responded that if it had, they did not notice, or "no." Two directors of physicians' offices reported that their system had crashed and that they had lost client information.

There were two centers that did have problems with their electronic systems. The director of Med-P02 discussed how her office lost all of their account information for their clients. Her office had been making electronic back-ups, but the system had not been working for three weeks when the fatal crash happened. This resulted in the director working "a lot of weekends" re-entering the information into the electronic system from the paper records. Similarly the director from Med-P03 discussed a virus that destroyed her client's medical and account information. This crash resulted in the office keeping paper copies of all of their records and doing additional electronic back-ups of their system.

Within childcare centers there were no breakdowns involving computers crashing and losing client information, but there was a case of the Department of Social Services' computers contracting and spreading a virus. The director from Child-P06 explained that the inspector arrived for her annual unannounced inspection and reported that her system was down because of a large computer virus that has spread from the Virginia Department of Motor Vehicle's system to the Virginia Department of Social Services' system. Because of this virus, the licenser had to do her inspection by hand and could not rely on any of her old notes (and sensitive client information). Instead, she had to ask for a copy of the prior inspection to verify that everything was in order.

Some salient points to highlight from these examples is that paper records serve, and continue to serve, as a valuable back-up for unreliable electronic systems. The first point is that all locations still had their paper files. This duplication of information means there is twice the work to do along with twice the information to store and secure. The second point is the invisible work of electronic system that results in an inability to determine if the system is still working correctly. The third point is that clients have little knowledge of when a crash has occurred and their information has been lost.

The director from Child-P06 explained it best. She explained that in general she believes that she is pretty technically literate, but she fully acknowledges that her system is mostly paper-based. She says this is because if she leaves for the day, when she comes back in the morning she can "trust" that the paper will be there. She says that if she relied only on an electronic version, she is not sure that over night her computer may "get a virus." She says that she cannot trust the "security and longevity" of the computer to manage everything for her.

## **4.7 Information Withheld or Hidden**

In offices filled with sensitive personal information, there are policies and procedures for accessing that information. HIPAA states that clients should have access to anything in their medical record and can receive copies. However, many directors of physician's office stated that patients would be provided sanitized versions of their file or reduced versions (e.g., the last two years of care).

Childcare centers do not have such a provision. All directors except one said that parents could access their child's file. However, access to the file was mediated with the parent accessing and reading the file within the presence of the director. The data provided in this section goes beyond trying to access the file to consider this issue further. It explores how people try to gain access to specific information and the conflict between open access and privacy.

### **4.7.1 Childcare Center Obscuring Information**

There were two incidents reported by parents where they believed that their access to information was denied. Both of these breakdowns were related "accidents." "Accidents," when used in this way, means that a child has been hurt in some way that results in harm to the child but not enough harm to result in a hospital visit. One type of accident is biting, which usually occurs with children who are under the age of three. This process can be traumatic for the children, but more importantly it can be upsetting for the vocal and paying parents.

In the two breakdowns parents explained how they were denied access to information about the identity of the child who harmed their child. In these cases the parents started asking more questions of the teachers and directors until the identity of the child was provided. One parent explained that this might not be in the best interest of the privacy of the child: "Some of the teachers would tell me who the child was and some wouldn't which I think the right thing to do would maybe be not to tell so I don't know."

### **4.7.2 Office Staff Hiding Information**

There were two observed breakdowns where information was hidden from other people in the center.

What is important about these breakdowns is that the centers manage and interact with sensitive information regularly. They leave files out, x-rays on counters, and shout client names, as discussed in other themes. Yet, there were still breakdowns where the participants desired personal privacy for their own information.

The first breakdown involved an office staff member hiding her timecard because she did not want others knowing "her business." The second breakdown involved mentors hiding their journals with notes about their peers.

### **4.7.3 Patient Confusion Over Procedure**

There were two incidents where patients called nurses expressing concern over not knowing enough information about their up-coming medical procedure. Both breakdowns

resulted because the patient had either assumed incorrect information about a procedure (e.g., staying up all night before a stress test) or was told incorrect information.

There is a lot of mystery surrounding medical procedures for lay people. Procedures are explained in confusing language usually with doctors speaking too quickly to understand what is happening. Add to the problem that patients are usually anxious, or generally not in a state to hear relevant information about a medical procedure, and patients can end up confused.

In relation to privacy, information about a medical procedure is perhaps the most salient information that a patient should have. The lack of knowledge reflects problems with the system for providing patients information about their care.

#### ***4.8 Local Negotiation of Content***

What is actually stored in a clients file is nebulous. For instance, one center discovered that one of their clients was a sexual offender. There was debate between the staff on how to document this discovery in the client's file. This example, and others discussed in this section, demonstrates that what can be considered as content of the client's file is not always clear.

To support privacy there were many breakdowns involving the negotiation over the content of a client's file. This may be because the childcare center director does not want to document the identity of the biological father, or because the doctor does not want to document information about a patient's test result. What makes it into the file is tenuous, debated, and layered.

##### **4.8.1 Auditing and Preparing for Incorrect Patient Information**

There were five breakdowns where the staff knew that they would receive incorrect information and prepared to receive it.

In this study the office staff would review information in a patient's file to make sure that it was correct. This was especially true in circumstances when the information was coming from people who were outside the office. For instance, the director of Med-P01, as observed in the two breakdowns, would review all of the information coming in from satellite offices. The director explained that she does this because it took too much time to stumble upon and "fix their work." Similarly, an office staff member at Med-P17 processed all of the payments so that they can be completed without any mistakes. The ladies at Med-P15 were also observed to constantly examine files that are coming in (e.g., faxes, transcripts, CDs with video files). The regularly found places in the documentation with incorrect patient information (e.g., client's gender).

The purpose of this auditing was to track information and to make sure that it is correct. For instance, the office staff at Med-P17 explained that after faxing over a letter to a school, she would keep a confirmation of the fax and put it into the patient's file. She did this just in case the school called to say that they did not receive the file: "A copy of the

fax is kept in their files in case the school tries to say that it was never sent. <The office staff> has printed out the letter to the school and it is on the left-hand side of her desk.”

This kind of file keeping and auditing is done because the offices recognize that mistakes can be made, and when they do happen, the center’s work may be compromised. This point is important. People were not auditing work for their own accountability, but to protect the client or the center as a whole.

#### **4.8.2 Filling in Missing Content**

There was one breakdown where an office staff member was observed to fill in information she officially was not supposed to modify. In this breakdown the assistant director modified the sign-in sheet that parents sign daily. This information is required by the Department of Social Services for the childcare center to remain licensed. The assistant director noticed that a number of parents had not properly signed-in or signed-out their child. Rather than leaving the spaces for signatures blank, she filled in the required information. She explained that she did this to protect her center, and because she knew that the children were currently safe (i.e., she saw them earlier that morning).

This action is against both the center’s and the state’s policy regarding documentation. It illustrates two issues: (a) the conflicting priority of parents to fill out sign-in and sign-out sheets, and (b) the conflicting priorities for the assistant director. In the moment when she realizes that information is missing she has to decide between citation and incorrectly filling in the information.



This means that the health care workers have to be careful about what is documented, even though they are encouraged to write everything down. For example, one medical director/owner said:

So even if it's taboo, of course we train our doctors to write it all down, write it all down. So that way you can always say look we dealt with it appropriately. What you can't do is if you don't do that... we always teach our doctors that you gotta look at, if we're in the court of law, can you explain what you did. And if you write it down then you got a record of what occurred.

To deal with these conflicting needs, health care workers cope through the use of layering notes. As discussed by two of the participants, they will layer their notes about clients using post-it notes to provide meta-information about the patient: "Sometimes we'll just let the doctor know if somebody's having problems like that we'll stick a post-it note on the front of the chart just to give him a heads up, and then we'll shred it." Tools like post-its serve a valuable privacy tool; they can be stored for the length of the problem, can be easily discarded, and are also easily identifiable for relaying information.

Childcare centers have similar concerns about not wanting to document everything about a child and their family. One reason is that childcare centers have a more open policy in regards to who could access client information. This means that there is a higher potential for more people to see problematic documentation. To deal with this problem the director from Child-P07 explained that she attempts to restrict access by functioning as a gatekeeper for client information.

The ambiguity over information allows for personnel to negotiate the formalized need for documentation while respecting the necessity for nebulous situations. Examples of nebulous information that directors listed as private yet documented include if a child is "difficult," marital problems between the child's parents, and the identity of a child's parents (e.g., "That's not really dad").

A unique reason reported for being hesitant to document information about a child is in cases of suspected abuse. Childcare center directors explain that they are "mandatory reporters." This means that that if they suspect child abuse, they are mandated to report the evidence to law-enforcing agencies.

The hesitation to document is due to the serious ramifications of the allegations being true. A child coming in dirty once can perhaps be an anomaly, but once there is repeated evidence, the directors explained that they have to start documenting the evidence. When the childcare center believes there is sufficient evidence, then they will turn over the evidence to someone in the Department of Social Services.

The conflicting needs to document cases of suspected abuse along with respecting the privacy of a child and her family is discussed in this quotation:

It's scary for us because you never know how a parent's gonna react and technically we're supposed to go to Social Services before we go to a parent, but you know what if there's a case where you know, you know family strife is going on, and it's very stressful right now, and what is the real story, is it a matter of frustration at the moment. You know was it a one time thing and so what's the right thing to do, really go to Social Services and risk the child being yanked from the classrooms, their home life, and an already stressful environment that will move on and be happier. Or, you know, go to the families first and say 'hey, we're noticing things and we're concerned for your family.

This quotation demonstrates that the director has discretion, and thus has privacy concerns over whether or not to document. If and when the director does document the suspected abuse it should be done in a way that respects the local needs of the situation.

#### **4.8.4 Not Providing “Necessary” Information**

There were three breakdowns where either physician’s office directors or parents discussed times when clients did not provide necessary information. In centers this breakdown occurred during enrollment.

When a client first joins a center there is certain information that is requested. For physicians’ offices, the required information includes prior medical history, insurance information, and information about the current malady. It also includes collecting information such as the patient’s social security number.

Directors reported two reasons for collecting a patient’s social security number, which could be considered a particularly sensitive piece of client information. The first reason is because some insurance companies use it as the primary key for locating the patient’s policy information. The second reason is because the center cannot reclaim lost pay through a collections agency unless they have the client’s social security number. Given these purposes, the physicians’ offices that were interviewed and observed attempted to collect all of their clients’ social security numbers.

Two physician’s office directors discussed breakdowns where they do not force their clients to provide their social security number. In these two breakdowns clients said that they did not want to provide that information and the center found ways to work around these special circumstances.

Only one parent discussed not providing their Social Security Number to their childcare center. They explained that they use the excuse of not having the number on hand: “Every time I handed in those forms at the daycares I say ‘I don’t know their’ or ‘I don’t have their social security number’s and they like said ‘alright don’t worry about it.’” These breakdowns demonstrate that even when information is mandated, there are still instances of negotiation over the collection of this information.

#### **4.8.5 Situations When there is a Need to Disclose More Information than “Normal”**

There were two breakdowns where a childcare director provided additional information to teachers for the security of the child.

At Child-P03 the director reported that she tries to use her personal judgment in unique situations. She explains, “It’s according to what it is, if I feel like they need to know it or not.” The times that she has had to use her personal judgment are custody problems, and for children who have foster parents. Both of these reasons are times when the identity of parents is critical for the protection of the child, thus requiring additional information to be disclosed to people in the center.

#### **4.9 Local Negotiation of Policy**

Policies appear to be binary; they are followed or they are not followed. However, participants reported breakdowns where policies related to security and privacy were negotiated. Examples are during cases when children were missing or when roles of people did not reflect their work that they actually did. These examples resulted in impromptu changes to the policy.

##### **4.9.1 Missing Child**

There were seven separate breakdowns where children were temporarily missing. All of the incidents that were observed occurred during transitions from the bus to the childcare center. This transition is difficult to coordinate because of the number of local variations. For instance, if the bus driver is sick then there can be a bus driver who is unfamiliar with which children to be picked up; if parents pick up their child for a special event; and, if children are sick and parents forget to notify the childcare center. These local variations lead to difficulties in tracking where children are and can result in children being temporarily missing.

The largest incident that was observed demonstrated the network of people who were involved in locating one missing child. In the incident the child was supposed to get on a bus after school, but she did not. When the bus driver tried to contact the child’s parents with the information he had on the bus, he realized that he did not have up-to-date information for that child. He then called the childcare center and talked with the assistant director. The assistant director then talked to the child’s teacher, children, the director, teachers at the sister childcare center, and the director at the sister childcare center. As the situation unfolded the director learned that the assistant director has not updated any information on the bus. The assistant director had been waiting for information from the sister childcare center.

In the process of still trying to track down a phone number an hour and ten minutes had lapsed. The mother called at the childcare center to report that her child was safe.

This breakdown involves numerous people and tools that would be difficult to account for without seeing this breakdown unfold. This includes the directors, the bus driver, the teacher, the child’s mother and father, children, and the sister center’s administrators. The

tools that are used are information stored on the bus, information known by the teacher, the laptops that store information, the bus book that stores who should and should not be on the bus, and a black box that stores contact information for parents.

An additional important point about this breakdown is the conflict between official policy and what actually occurred. This childcare center has a policy about reporting when a child will not be on a bus or will not be attending the childcare center that day. The director explains:

Well, it's lots of little lives, you know I tell people all the time with the track down policy, we charge them \$5 every day that we have to call them to track down their child. We bill it to tuition to make it a true payable thing, it's not a courtesy. But, what's scarier, the parent losing the child, or the teacher losing the child? I was like, you can sue us... you can be mad at yourself, but you can sue us, and that's just not a risk we're willing to take.

This policy was created to try and mitigate incidents like the one presented above. Other childcare centers had similar policies yet only one other center reported charging money for a policy violation. Yet, there were six other incidents where the location of a child was not known.

#### **4.9.2 Inappropriate Disclosure of Incorrect Patient Information**

There were three incidences of divulging patient information to the wrong person, thus breaking the policy of patient confidentiality.

In larger practices familiarity with every patient is not possible. Instead, a larger reliance on patient charts and documented information is necessary for the continuous care of patients. This can mean that for some health care professionals the differences between patients can become blurred, and mistakes can be made when associating one patient's information with another.

Two of the breakdowns observed involve listing an incorrect patient's name to another patient. These are small problems and not as problematic as the third breakdown. The third breakdown involved an office staff member drafting a letter to a client about their medical situation, and then sending the letter to the incorrect person.

Regardless of the size of the privacy breach, it is easy to imagine a scenario where the context of the work becomes separated from the tools people are using. For example, in the case where the letter drafter was told to write a letter but then became confused about which patient she was to draft it from, she was working across the paper file system and two electronic systems. The number of systems she was cognitively organizing easily allows for people to become confused and make mistakes that lead to privacy violations.

#### **4.9.3 Licensing Problems**

There were seven incidents related to licensing. Licensing is the state-mandated process for regulating childcare centers. One of their responsibilities is to make sure that

childcare centers are managing the child's information in a confidential manner. There are two incidents that demonstrate this process that occurred within Child-P01 and Child-P03.

The licensor for these sites is the same person, PD1. PD1 primarily works from home and she drives to different centers to do scheduled and unscheduled visits. During these visits she tours the childcare center and then looks at ten percent of child and staff files. Any citations issued are posted on the DSS website. An example from Child-P06 is included below:

Facility Type: Child Day Center  
License Type: Two Year  
Expiration Date: Feb. 21, 2011  
Administrator: Child-P06 Director  
Business Hours: 7:00 A - 5:45 P, Monday - Friday  
Capacity: 130  
Ages: 1 month - 12 years 11 months  
Inspector: PD1

Inspection Date: Sept. 17, 2009  
Standard #: 22VAC15-30-610-D

Description:

The last evacuation drill noted was for the month of April 2009. These drills are required to be done monthly.

Action to be Taken:

We will use the monthly desk calendar as the reminder to perform the drills. We will pre-mark the calendars now and continue to do so for the upcoming years to ensure compliance is maintained. We will also conduct 2 drills per month, for a few months, to ensure the children/staff are familiar with the process.

In this citation the childcare center had been reprimanded for not doing evacuation drills as frequently as necessary.

Additional citations were issued to the childcare centers that were studied during the times of observations. These include problems such as a child being locked in a closet, the lack of an authority statement, playground equipment not meeting standards, missing information in staff and child files, and missing children.

The breakdowns that were observed indicate places where there was a conflict between the official policy and what actually occurred. In these incidents citations should have been issued, but were not.

In the first breakdown, Child-P01 is visited for an unannounced inspection. In this inspection the licensor observed three problems that should have been reported: (1) chemicals in a cabinet that are not locked, (2) files that were not updated, and (3) purses

that were accessible. The reason that this childcare center was not issued a citation could be attributed to the prior relationship between the director and inspector. It was revealed through the observation that the director and inspector used to work together. Below are observation notes of a discussion between the licensor and director:

‘and, you've got your emergency documents on there for your bus and your van route?’

‘emergency documents being...?’

‘who you're transporting, sign in sign out, emergency information, first aid kit?’

‘first aid kit's on there, notebooks with all the contact information's on there . They have a list downstairs the other of messages as well as up here that they check to cross-reference with their cross-off list of who to pick up, as well as their phone numbers. They do not leave the school until they contact <inaudible> despite the school saying 'yes' they were a car rider’

‘do they keep a list of who's on there at the given moment, like a check off like 'we have 16, and it's Johnny, Jane,’

‘They have a laminated list, itemized per vehicle as well as... I wish I had it handy, but a laminated list with all the children's names on it that they can use a white erase marker, and cross off who's not supposed to be attending’...

This last conversation was a little bit of a struggle for PT1. She seems to know that they are not implementing all the procedural requirements on the bus. None of the explanations she has given me or even PD1 here have included a current count of who is on the bus. And, there’s apparently no sign-off to signal that no children are on the bus after the route is complete. PT1’s answer to PD1’s questioning of whether this last check even takes place, regardless of sign-off, seems a little nervous and unconfident. In her roundabout explanation of the cross-off list, which avoids directly answering the question, PT1 admits that there is not a count/list of who’s on the bus at any given moment without directly saying it... PD1 has already noted the purse on the child-accessible, unlocked shelf and how she dismissed closer inspection for social reasons. We later learn that she overlooked a can of spray chemicals in an unlocked cabinet in the art room, and an unprotected outlet. Finally, she was made aware that files were not fully updated and said that she would turn the other cheek as long as she didn’t see PT1 actually updating the files. In the end of the day, no violations were reported in the final write-up.

In the second breakdown, the observer shadowed the assistant director from Child-P03 as she went to a teacher’s room. During this visit the assistant director made sure that the teachers were compliant with VDSS requirements. In one room the assistant director noticed many problems and made the teacher aware of them.

What is particularly interesting in this breakdown is how the assistant director has a condensed one-page list of problems that she should attend to compared to the three-page

list that is provided by her licensor. The difference between the official policy and local policies is highlighted in this artifact.

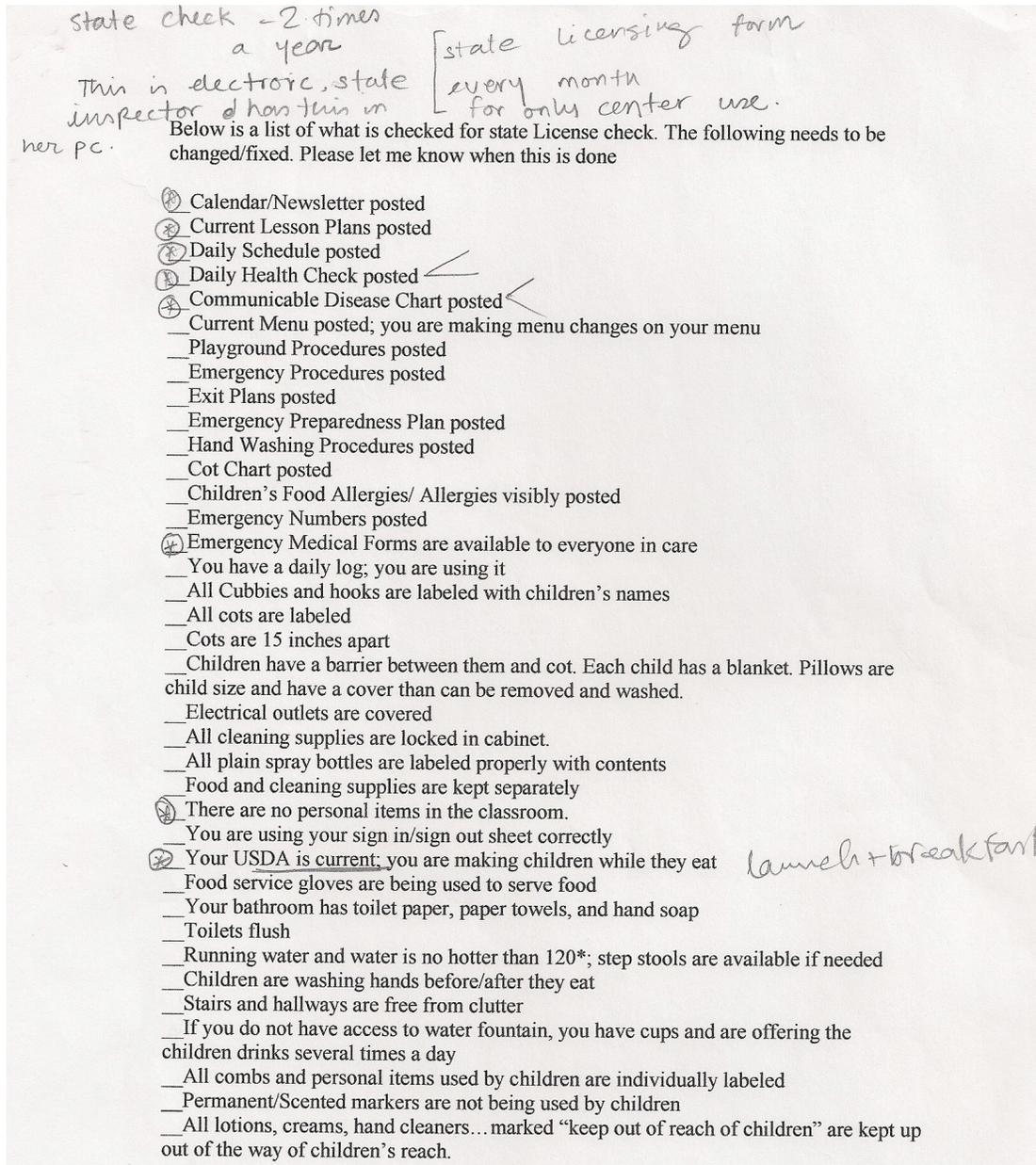


Figure 18. The one page condensed version of interpreted licensing requirements.

Negotiation over what constitutes as a violation in childcare centers was local to the relationship between directors and their licensors. For example, the director from Child-P04 regularly contacts her licensor to determine how to instantiate policies. She says, "I tend to, you know 'this is what it says and before I deviate from this, you know I'm going to ask someone. I'm reading it this way is it really ok to do it this way?'" So, there's a lot of times I'll call the licensing specialist and get her opinion."

#### **4.9.4 Pharmaceutical Representatives & Insurance Companies Seeking Patient Information**

There were three incidents involving pharmaceutical or insurance company representatives were seeking information that the director that could be perceived as private.

Pharmacology representatives visit physicians' offices regularly. As documented by Craig & Stitzel in their book "Modern Pharmacology with Clinical Applications," in 2004 eleven billion dollars was spent on "education" and "marketing." This involved providing "educational" lunches for the office where the pharmacology representative talked about their drugs. In the centers that were studied, there was a time where four pharmacology representatives visiting at a single hour. It was normal for pharmacology representative to drop off free food to the office staff and then talk with the doctors or directors.

One particular incident illustrates how local policies can be in contradiction to privacy. In the breakdown a pharmacology representative was visiting a physician's office for a "lunch and learn." During this lunch and learn the pharmacology representative was able to fax over all of the relevant information from a patient's file to her office. While it is unclear if this is against the practice's privacy policy, the patient was not contacted. The pharmacology representative was observed going through the file. This information was then sent off to another set of people who reviewed the information for their purposes. From observing the reactions of the people in the office, this action was not unusual.

In the other two breakdowns people who work in the physician's office expressed concerns over why an insurance company requested copies of a marriage certificate and other information about the client. The directors explained that they do not believe insurance companies should have access to that sensitive information. One of the participants reported that he would not work with certain insurance companies because of information they request about his patients. He does not believe the requests to be "ethical."

#### **4.9.5 Receptionist Functioning as Nurse**

The nature of small physicians' offices is that there is a lot of work to be done, and not many people to do it. This means that nurses and doctors sometimes have to answer the phone, pull their own patient files, and do work that is not associated with their official "role." For example, the director from Med-P19 says, "I don't really believe in job descriptions for that very reason, because everybody needs to do everything and know everything. That's the only way it can work in this day."

Everyone lends a hand at whatever job is necessary for the function of the business. This leads to receptionist finding cases where doctors have prescribed a procedure that might kill their patient (as observed at Med-P15), doctors making copies of papers and collating them (as observed at Med-P16), and doctors delivering mail (as observed at Med-P17).

The breakdown in this situation occurs when people in the office do work that they are not allowed to do. This was only observed once at Med-P15. In this breakdown the receptionist was observed to be writing prescriptions. A nurse saw the receptionist writing the prescription and while she does not take away the prescription pad, she reminds the receptionist that she is not supposed to do that.

#### **4.9.6 Staff Catching Incorrect Medical Procedure**

There were two incidents where someone who was not a doctor caught the doctor prescribing a test that could have killed the patient.

Patient files are reviewed at different times in the lifetime of the file. Staff were observed to review a patients file when it was first pulled, when the patient called for an appointment, when the patient called with a question, when a fax came in for a patient's file, and when the file came back into the office after the patient had been seen by the doctor. These times serve as important places to review updates and changes to the patient's file.

Breakdowns happened when during the review process the reasoning behind a choice is not explained, and the procedure looks incorrect. In the first breakdown a nurse asked the receptionist to set up a surgery for a patient at the hospital. Off the top of her head, the receptionist recalls that the patient had the same surgery recently. When the office staff conducted a further investigation, they realized that the receptionist was correct. What they decided to do, with the help of the office director, is to schedule the surgery for a week and a half from the current date. This provided enough time to cancel the appointment. The receptionist explained to the observer that a surgery so close to the last one would likely have killed the patient.

In the second example, also from Med-P15, the echo cardiologist catches another time when the doctor ordered a stress test on a patient who had recently had a heart attack. While I was not able to watch how he noticed that mistake, I was able to notice that he went to the outpatient window to talk to the receptionist, and called to cancel the test immediately. The office then took care of the paper work in the patient's file.

#### **4.10 Access Policy**

Access to client information was found to be relatively open, as discussed earlier in this chapter. However, there were times when people in the socio-technical system restricted access to necessary client information. Two examples of restrictions is discussed in this section.

##### **4.10.1 Parental Over Restriction of Access**

There were two breakdowns where parents designated that no one could access their child's file.

Child-P01 and Child-P04 both are NAYCE accredited childcare centers that elicit permission from parents about who can access their child's records. An example form is

shown in Figure 13. Both childcare center directors reported that some parents indicate that no one can access their child's information, including the director.

The response from the directors demonstrates the negotiation of policy. When asked how they respond to that particular situation the director explained that she would discuss with the parents what their concerns are and try to negotiate a case-by-case agreement. For example, a director explained, "I go up to them like 'k, so you're saying the director can't look at that, that means I can't prove your paperwork, can you please you know understand that my role is this...."

Some information, like allergy information, must be listed in the environment for others to access. Therefore, parents restricting access can actually be harmful to the care of the child. Further, without being able to display relevant information, the child would not be allowed to attend the childcare center. One childcare director explained, "The teacher's need that information because it includes, you know, the emergency contacts, allergies that the child might have. Those are some crucial pieces that the teachers have to know."

#### **4.10.2 Restricting Client Access to Files**

There were eleven incidents involving centers restricting client access to their files.

There are laws affecting client access to information. For example, HIPAA stipulates that patients are allowed to have access to their files. While there is not a similar law allowing parents access, parents expressed that they could access to their files (even though none had asked to look at them). However, when discussing with childcare center and physician's office directors a client's ability to see their files, many directors explained that client access was limited.

In the most complete description, the director from Med-P01 explained that patients were not allowed to see their file because they would not understand the information. At this center the client would not even be provided a copy of their file if requested because the director said that she wanted to prevent the client from losing the record. Instead, the director said that she would mail a copy of the file to next physician's office that the patient was attending.

This policy of limited access was actually observed. A child had finished his course of treatment, and when the father asked for a copy of the files the office staff explained that they would happily mail on a copy, and provided a father with a copy of their address.

Other reasons provided by directors of physicians' offices for not allowing the client full access to their files were that patients would not understand the record ("They don't understand what's in their record"), because the technology does not currently support sharing the information between the office and client, because the client does not actually own the information ("The information in a file belongs to a patient, but the file itself belongs to the doctor"), because they do not want to lose their original record ("We never release the physical file"), because there might be information that the office does not want the patient to see (e.g., being obnoxious), because the patient does not need to

see all of the information but only a summary of what has been done (“We don’t give them the whole file; there’s a limit to a one page thing”), and because the patient should only have access to a copy.

Different from physicians’ offices there was more of a spectrum over what parents could and could not see in their child’s file. All childcare centers except one, Child-P02, said that parents could come in and view the child’s file within their office. This was usually with supervision from the director (“They just need to ask for permission to get to it then we literally pull it out for them and we’re standing right there with them”). While this appears as more open, the director explained that she would usually stay in the room with the parent when they were looking at the file. This surveillance created a kind of restriction for the parents being able to thoroughly examine their child’s file.

This surveillance serves a purpose. Childcare center directors explained that they would sometimes keep sensitive information towards the back of the file. The director of Child-P02 said that the reason she would not want parents to look at their child’s file was because she had made notes about the child or parents that she would not want them to be able to see.

While parents were not restricted from examining their child’s file, there was other information in the childcare center that parents could not access. These include the logs that teachers keep in their rooms of daily activities, videos that were kept and stored of a child’s activities, and logs of suspected child abuse.

#### ***4.11 Sensitive Information Publically Accessible***

Given the diverse uses for client information, sensitive information is dispersed and left in the open environment. This includes sensitive information being left on counter tops, pictures of children on Facebook, posting sensitive information on the walls of childcare centers, shouting client names, and taking sensitive files outside of the office where they are not secure.

Information in these places does not necessarily indicate a breach in security, but reflects the uses of sensitive information that are not accounted for with current technology systems. These uses reflect a kind of circumvention of the system to support work practices.

##### **4.11.1 Open Access to Client Information**

There were fifteen breakdowns where office staff had open access to client information.

In all of the observed physicians’ offices the patient’s files were openly displayed for anyone in the office to access. An example is shown in Figure 19 from Med-P01 where the files span the office space of the medical director and staff. These files hold highly sensitive information. The fact that they are freely available for anyone to be able to access makes them appear to not be secure.



Figure 19. Med-P01's client files open for anyone to access.

Perhaps the most representative quotation comes from the director at Med-P08. When asked if anyone had ever accessed information they should not access, she said, “I don’t think so, because most of the stuff that we have here is just stuff that we can always access, so there’s not really anything we can’t get into.”

Even more indicative of the issue at hand, people in really small offices know who is accessing information because there are a limited number of people. When the director of Med-P10 was asked who accesses all of the patient’s files she said, “Both of us do, yes.” When there is only one other person modifying patient information, it is obvious who the other person is.

Childcare centers also had similar breakdowns. They also kept client information in unlocked locations, which is against VDSS policy. While the files in childcare centers are usually stored within drawers of filing cabinets rather than on shelves like physician’s offices, access is almost as readily available.

Many of the childcare centers reported that the child’s files were stored in locked offices or within locked filing cabinets. However, this was never actually observed. Within three of the childcare centers that reported that they locked their files, a key was never used and the observer checked when the director was out of the office that the drawers were unlocked.

Open access to client information has many functions: the files are easier to access when the office becomes busy; it keeps what work needs to be done visible; and, it signals to new clients that they already have repeated successful business. However, it also means that the information is more available to steal.

#### **4.11.2 Patient Information Left in the Open**

There were two incidents that pertain to client information being left in the open.

Patient information is ubiquitous at the physicians' offices that were studied. It is on every desk, on post-it notes, and in files physically surrounding the office staff. With all this information about it is easy for patient information to be left out of a patient's file, or for a patient file to be left open where anyone can walk around and view the contents. The director from Med-P18 explained about people entering the office and the impact of having open information: "Because obviously they are going to come in and see things laying on the desk that pertain to patient information."

Similarly, during an observation the observer noticed a client x-ray that was left on the counter that was detached from a client's file. A nurse came over, picked up the x-ray, looked at it, and then put it back on the desk. The nurse noted that there was no identifying client information on the file.

Leaving information open makes the work visible. However, it is in direct conflict with keeping the information secure in the sense that it is not locked away and protected from prying eyes.

#### **4.11.3 Children's Pictures on Facebook**

Two parents discussed an incident where pictures of children were on teachers' Facebook profiles.

In this breakdown a parent had discovered the pictures when she became "friends" with the teacher on Facebook. The problem was resolved by having the pictures removed from the profiles, along with changing the policy about posting pictures of children on the internet.

Two or three of the teachers had friended me on Facebook. An a week later in looking at their Facebook I noticed that they had pictures of the children playing in that I daycare on their Facebook. So, that afternoon, I called the daycare and told the director. It was like three o'clock in the afternoon. Then when I got there to pick them up the owner was there. So she pulled me aside and apologized and said that it would get fixed. And they brought all the securities, teachers into the office and watched them take the picture down off from the internet before they left that day. So, they are definitely on it as far as fixing the problem and that's the feeling of nervousness that I have. You know just like very personal pictures are up.

#### **4.11.4 Client Files Dispersed in Environment**

There were eight breakdowns where information was dispersed in the environment.

Information about children was observed to be in many places in the childcare center. For instance, one childcare center had separate paper files for the VDSS required information, for accident reports, and for documenting sensitive information. Childcare center directors also discussed that there were files kept about the children in each of the rooms

that the children spent their days in. Two childcares, Child-P01 and Child-P04, also kept books documenting a child's developmental progress that were shared with parents.

Apart from large files of information, there was also information about the children and their families in family directories, rolodexes, in running journals of what was going on in the center or each room, in daily write-ups of activities in the room, on display boards, on sheets for dietary concerns, and on post-it notes with names and contact information.

The ubiquitous distribution of client information in childcare centers was salient. This is demonstrated in Figure 20.



Figure 20. Six pictures depicting the places where information about children is stored, starting from top left moving clockwise: bulletin boards, rolodex of contact information with a notebook of absent children, a description of activities in a classroom, desk of

assistant director with quick access information and client files, taped up papers of illnesses and inspections, and binder filled with documentation for a classroom.

Client information can also be dispersed due to local need. For example, the director from Child-P01 discussed how when her center first opened child files were all over her office because she “needed” to have them out: “We had a mass enrollment of about 200 children, so I was processing paperwork and I had piles on my floor. And, so when the kids were coming in, I was like 'oh my gosh.’”

Similarly, the licensor for many of the childcare centers in our study explained during an observation that information about the children should be locked up in a filing cabinet to protect the privacy of the children. However, not all information can be locked up. She went on to explain that she recognizes that to be able to properly care for children information has to be displayed in the environment (e.g., allergy information).

The problem related to security is the lack of available information about the real practices. When parents ask where their child’s information is stored they are shown a locked filing cabinet that only a few people can supposedly access. This creates a false pretense about how distributed the information actually is. This is not to necessarily say that the childcare centers are not keeping the information secure. It is merely stated to note that there is ambiguity surrounding how information is being actually being managed.

#### **4.11.5 Disclosing Patient Information**

There were six breakdowns where health care personnel were observed disclosing client information in a way that violated HIPAA.

The people at the centers were aware that they were stewarding sensitive personal information, and took precautions where they saw appropriate. However, there were still times when an office employee would overly disclose personal information either by accident or without knowledge that what they were doing was a violation.

In the first breakdown the director from Med-P01 created a booklet for a new patient, and she needed the patient’s name and address. Because the file for this patient had already been taken through to another room, the director walked over to patient room, which held approximately 10 people in it, and asks the patient for her name and address. The information is verbally disclosed by the patient loud enough that everyone in the room was able to hear.

This breakdown highlights a clear lack of standardized rules surrounding what is considered private information, and what is not. In this case, the patient’s name and address is not considered private by the office, while it is declared as private by HIPAA.

In the second, third, and fourth breakdowns, a health care worker shouted out a patient’s identifying information even though there was a local rule surrounding disclosing identifying information. In the fourth example, people at Med-P15 realized that the fax number that they had for faxing a patient prescription was incorrect. They had been

faxing numerous copies of prescriptions and sensitive information to the wrong number. The last example involved providing information about a client without written consent (and is explained in more detail in the section on HIPAA).

#### **4.11.6 File Being Kept Outside of Office**

There were six breakdowns involving client files being kept outside of the office.

There simply is not enough space at centers to store all of the client records. For that reason, many records that are past a certain span of years are moved to a secondary location that is outside of the office.

Moving files to an offsite location has two important points in relation to security. The first is that the files are stored in locations such as basements (e.g., “He keeps them in his basement”), central storage facilities (e.g., “We have a central storage room”), and “storage.” All secondary locations bring in a new set of stakeholders who now have access to a client’s files. Examples include people such as the physician’s family. The second point is that electronic files also introduce a larger spectrum of people who can have access to the private information in the process of creating back-ups.

All physicians’ offices reported keeping files for at least up to seven years. Files over a year were typically moved to an additional storage location, and files over 7 years were usually moved off site.

The directors of Child-P03 and Child-P01 were the only childcare centers who reported destroying all or part of their files after a child was no longer in their program. For example, after children no longer attended the center copies of their birth certificate were destroyed. The remaining childcare centers reported that their files would be stored indefinitely. Many of these childcare centers used external locations to store their extra files.

The reason for indefinitely keeping a child’s files was best summarized by the director from Child-P03. She explained that it again comes down to children being a protected class of citizens. While she would hate to think that any child was ever abused within her childcare center, she needs to have the documentation ready to support whatever problems may occur in the future. One childcare center director said that he kept all of his child’s files because it was required for licensing (which is not true).

Both in childcare centers and physicians’ offices people were observed to take files home where additional people could access the information. For example, Med-P16 had a doctor with a “homework pile” that he took home with him each night to do things like calling patients to make sure they were recovering well. The director from Child-P03 also reported that she had files in her car.

#### ***4.12 Synchronizing Information with Reality***

When managing client information there were problems in regards to information reflecting a correct objective reality. For example, the problem of not having correct and

up-to-date information about a client could manifest in a missing file (e.g., client name change).

Additionally, directors were observed to gather information about a client that was not within the client's file, for the purpose of a greater understanding of the clients. In some cases, these actions were found to infringe on the privacy of the clients.

#### **4.12.1 Difficulties with Client Care when Outside of the Center**

Three breakdowns occurred where the directors had difficulties managing client care when the client was outside of the office. These breakdowns represent a boundary between the client and the center where the center wishes to gather more information about the client.

In the first breakdown the director from Med-P16 had to manage the care for a patient after he left the office. The patient told the director that while he can remember his appointment, it is a lot to remember for him to get his prescription filled before his appointment. He explained that it involves him remembering a few days ahead of time to call the bus, go to the pharmacy, get the prescription filled, call the bus, go home, and then to remember to take the medication the day before the appointment. He says that this is difficult for him manage given his age. The director put a mark in her calendar to remember to call him, but this message is not contextualized with the patient's medical record.

In the second example the director at Med-P19 reported having to deal with patients who have been using the office to gather prescription drugs. While it is in her office's best interest to make sure that the prescriptions are not being used illegally, in this case she is trying to maintain the care of that patient to make sure that when outside the office they are using the prescribed drugs adequately and appropriately. Currently, she has to go outside of the electronic record system to verify that the patient has not been abusing their prescriptions.

The last example, a childcare center director reported that she desired to know more information about children who are having developmental problems. She reported that parents are not providing her enough information, but realizes that parents "want to see their child as a certain way."

#### **4.12.2 Getting Information that is Purposefully Not in the File**

There were two breakdowns where the office staff workers gathered information about a client that was purposefully not put into their electronic file.

In these breakdowns the person who was being observed handled the processing all of the incoming payments from the satellite offices. As payments came in, she went through the normal workflow of entering the services, totaling the bill, submitting the statement to the insurance company, and entering any payments from the patients. During this workflow some patients ere flagged as having a note in reference to their file.

In one breakdown the office staff member reviewed a note indicating that there was something unusual about the client's file. The woman found that the note was insufficient to answer her question. In this case she called the woman who was in the basement. This woman has special access to specific information. Through discussing with the woman in the basement, the woman being observed has all of her questions answered.

When asked why more information about the patient's circumstance was not in the file, I was told that it is not everyone's "business." This means that the file was purposefully fragmented to protect the privacy of the patient.

#### **4.12.3 Incorrect or Unresolved Information in the Patient File**

There were four breakdowns where incorrect or unresolved information was discovered in patient files.

These breakdowns include a receptionist discovering that another person in the office had entered "joke-like" information for a client's address, the director discovering that she did not have a patient's updated phone number, the director discovering an incorrect gender was associated with a patient in her file, and the director not having updated insurance information for a patient.

Over all, these breakdowns were encountered because the director scanned the file and noticed that information in a client file was incorrect. Supporting this kind of scanning is invaluable, and can go far in making sure that other information in a client file is correct.

#### **4.12.4 Looking Up Patients on Sex Offender Website**

There was one breakdown where nurses and office staff from Med-P15 looked up their clients on an online sexual offenders database.

The circumstances are somewhat unusual. Earlier that morning a nurse read in the local newspaper a story involving one of the center's patients and an underage minor. This sparked a desire to see if any of the other patients were sexual offenders. The office then proceeded to enter their client's names into the online sexual offenders database until they found a second person.

What resolved was a discussion about client care in the face of this new knowledge. The nurses and office staff agreed that no one knows "the whole story," and that perhaps their clients were innocent.

#### **4.12.5 Lost Paper Patient File**

There was only one breakdown where a physician's office director reported that when client files were missing that he "will then recreate the file." This is perhaps because this center was also the only one that only used paper files.

What is valuable about this quotation is also what is missing from it. He does not notify anyone that the patient's file is missing. He particularly does not notify the patient.

#### **4.12.6 Missing Client Information**

There was one breakdown where missing information about a client was brought to the attention of the nurse.

In this incident, the nurse called a patient to update the medication dosage. However, in discussing this change with the patient, the patient explained that she had already been told to change her medication to that dosage. This change had not been documented in the patient's file. The nurse hung up the phone, and made the change in the file. She reflected upon how dangerous this situation could be. For instance, a wrong dosage could result in patient harm.

#### **4.12.7 Missing Documentation to go into a Client File**

There were four breakdowns where client information was noted as missing.

Information that ends up in the client's file comes from numerous locations. For instance, information may come from forms filled out by teachers in rooms, or from nurses entering in information during a patient visit. The diversity of locations can result in problems recognizing when information is missing.

Breakdowns that were observed involved patient mail not being passed on to the correct person; annotations about a patient not being placed in the file; missing transcriptions; and, missing doctor signatures needed for a patient's medical procedure.

#### **4.12.8 Missing Electronic File**

There were four breakdowns where participants were not able to locate an electronic file.

The creation of electronic patient files was observed to be reactive rather than proactive. The staff in the observed physicians' offices only created an electronic file when there was a direct need to document information about a patient. For instance, at Med-P01 a new electronic patient record was only created when there was a need to schedule the second appointment for the patient. Alternatively, Med-P16 would create the electronic file almost immediately because she wanted to verify if the patient could have their appointments covered by insurance. And, to show another perspective, Med-P15 only created the electronic file when the patient was scheduled to be seen by the doctor.

In the three out of four breakdowns in this category, the breakdowns occurred because the patient record had not yet been created. In the first breakdown, a patient was seen over the weekend when no one was in the office to create the electronic record. The second example involves a health care worker entering information about a visit prior to the electronic record being made about the client. The third incident involves a patient calling the practice for medical advice prior to the first visit.

In the fourth breakdown is different than the previous three because it is due to a problem with a file that has already been created. In this breakdown a nurse was not able to look up a patient in the EMR system based on their name. The receptionist recalled the

patient's ID code off of the top of her head and told it to the nurse. This allowed the nurse to look up the patient.

#### **4.12.9 Permanently Missing (or Dead) Client**

There were four breakdowns where physician's office directors tried to determine why a client was missing.

At a physician's office, if the patient does not show up for appointments, they can become lost in the daily work of the centers. There are times, however, where the center tried to locate a patient to either try or schedule a new appointment or to collect payment. A breakdown occurred during these times because the patient is not reachable. This is a case where the office maintained sensitive personal information about a client, but the client had severed the relationship.

In the first breakdown at Med-P17, two office staff members were observed to interact with both the electronic and paper record to try and locate a child. This child was missing but the office needed to pass along a message to the patient's parent. Within 30 minutes the staff members had talked to enough people to discover that the patient had moved to live with her father, had acquired the father's phone number, and located the client.

In a second breakdown at Med-P17, an office staff member used health insurance portals to locate patients who were missing. She explained that patients often notify their insurance company when they have changed location, but they do not always notify their physician's office.

In the other two breakdowns both directors from Med-P16 and Med-P17 discussed a patient who they knew was having severe medical problems. These directors were trying to determine if the patient had not attended their last appointment because they were sick or possibly had died. The director at Med-P16 went so far as to contact the patient's general practitioner to make sure that the patient was doing well.

#### **4.12.10 Recalling Codes**

There were three incidents where entering codes into the electronic record system resulted in incorrect information being associated with the client.

Users had problems recalling codes from her memory. This resulted in the participants using incorrect codes when interacting with a client's electronic file.

The first breakdown involved the director at Med-P17 using the system shown in Figure 21. In this system the user has to type in a code to associate the procedure the patient had to the file. This allows the staff to then bill the insurance company for the procedure. In this breakdown the user was observed to type in incorrect procedures, recognize her mistakes, and delete the incorrect procedures.

The second and third examples involved staff from Med-P01 not being able to recall the necessary codes. Because of their inability to recall the correct code they spent time with

the EMR associating incorrect information with the patient’s file that had to be cleaned up later.

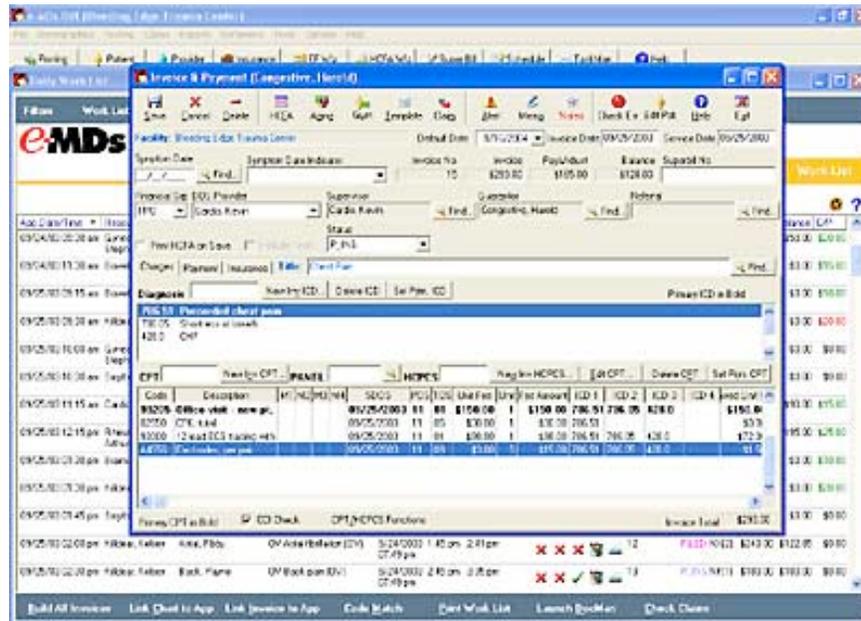


Figure 21. Med-P15’s electronic file system called “e-MD.”



Figure 22. Med-P01's electronic file system.

### 4.13 Summary

The breakdowns presented in this chapter span multiple kinds of phenomenon. There are breakdowns that were minor, such as interface problems, and there were problems that were life critical, such as detecting an incorrect medical procedure. Additionally, there were problems where policies were broken in a minor way, such as when staff publicly

asked for a patient's address, and times when policies were broken in a major way, such as when a child was missing.

These breakdowns are analyzed in Chapter 5 in reference to three topics to deeply engage in what the experience means in reference security and privacy.

## **5 The Phenomenon of Security and Privacy in Managing Sensitive Client Information**

In the previous chapter the breakdowns relating to security and privacy of a client's sensitive information were presented.

This chapter synthesizes these breakdowns with three different lenses. These lenses are used to present the essence of what security and privacy mean in social, negotiated, and technical spaces.

In the Section 5.1 on Privacy and Security Embodiment I examine what security and privacy are and are not embodied within. Section 5.2 then explores how Communities of Security can move beyond considering security as an individual anomaly, but instead considers how security and privacy are constructed through mutual collaboration. Section 5.3 on Zones of ambiguity last considers what security and privacy mean in interpersonal and ambiguous situations.

Each of these lenses represents a metaphorical prism in an attempt to capture and re-examine privacy and security.

### ***5.1 Privacy & Security Embodiment***

During all interviews and observations of childcare centers and physicians' offices there was only one breakdown where a participant discussed a threat that was not prompted by the researcher. For example, many questions asked the participants who could access information under certain circumstances. However, in all observations and interviews, there was only one time when a participant raised a threat that was not previously discussed.

To explore this threat and its relation to security embodiment, I present summaries of breakdowns that were presented in the previous chapter as possible choices: was this unprompted reference to a threat an allusion to the computer system contracting a virus and losing years worth of client information; was it in reference to seventy years of client files being stored in the basement of the doctor's house where anyone in his family could have access; or, was it in reference to the general lack of password usage, or, even shouting passwords in the workspace. It was when a director talked about a man in a red bandana who liked to spend time hanging outside of a childcare center to try out his latest pick-up lines on the pretty teachers. This point demonstrates the tension between the perception of threats versus actual threats.

In the breakdown where the director talks about the man in the red bandana, the director turned to me. She sees me looking at this man who was spending an awfully long time trimming the grass. "Oh him," she says. "He is always hanging around here trying to talk to us." After explaining that this troublesome man is "creepy," she says that she does not see the need to call his boss, because he is not a serious "threat."

This breakdown raises the question, what is considered a threat to childcare centers and physicians' offices? If a man hanging outside a childcare center is not a serious threat, then what is? And, further than asking only about threats, where is security and privacy situated within the work that people do? Is security and privacy used because of perceived threats, or for some other reason?

In this section I discuss the data presented in the previous chapter in order to reflect on how the people in these spaces embody security and privacy into their every day work and examine the construct of a “threat.”

Security researchers are preoccupied with threat models. A threat model is a model of who and what a designer should be concerned about in reference to an attack. For instance, I have used the following threat model to situate the work presented in this dissertation:

*“In these domains the adversarial actions are unintentional, unwelcome, and intrusive access and modification of sensitive personal information. Examples include medical and childcare center personnel, medical researchers, and insurance companies accessing patient or child information that should not be available (i.e., private). A second example includes ‘work-around’ practices of the personnel themselves that results in unknown and insecure information disclosures.” (Vega et al. 2010)*

Threat models, like the one presented above, indicate who or what is going to attack the assets (e.g., external and internal people), the assets that need to be protected (e.g., the client’s private information), and the mitigating mechanisms to protect those assets (e.g., some social/technical system) (Howard 2005). With these tools, threat models provide a lucid representation of security and privacy: security is the defense against external attacks; privacy is the desire to keep something hidden, thus requiring security.

Threat models allow for designers to determine their defense, and in accordance with that defense the priorities of managing an attack. They are much like drawing a schematic of a defensive wall surrounding the royal jewels stored in a castle’s towers. With a threat model in hand, the designer feels empowered to fight against the forces of evil with the sure knowledge that they have thought of all unfavorable circumstances.

The problem with threat models is that they account for perceived threats. They are, in essence, plans. Plans, which are reflected in computing systems, threat models, and designs, are unfortunately fallible (Suchman 1987). This is because, to quote Bellotti and Sellen, “computing systems are only secure in *principle*. They are rarely secure in *practice*” (Bellotti et al. 1993).

Plans account for the accountable, taking small heed of actual practice, which can appear as a busy and noisy mess. This is why when put into practice, plans can come undone in the face of local circumstances, changing needs, and unexpected events. Designers need to not only use plans, like threat models, but also need to account for work practice.

The work that people do is where security and privacy actually exist. The threat model exists as a tool, as does the protective fortress. The real work in protecting and interacting with assets is in the field and in the daily actions that are taken in reaction to local circumstances. It is in the moment when the parent says for the fourth time that they have “forgotten” their child’s social security card, where the childcare center director has to press for the information or respect the privacy of the parent. It is in the moment when a co-worker comes over to ask for the password for the hospital’s EMR system that the health care worker has to assess if it is important for the work to be done or for her password to be protected. And, last, it is in the moment when a teacher documents instances of child abuse in the back of a file where no one else can access it. It is in these moments where security and privacy comes into play, and threat models are not as apparent. Where is creepy lawn care worker in each of these situations? He is simply not there.

By examining actual practice, and where those practices breakdown, we can examine where security and privacy are embodied. The embodiment of security and privacy into the work that people do represent the places they are valued and the situations that security and privacy can be designed for.

In the following sections I discuss the data with the following framework. I ask the questions, “What rules are broken or uninstantiated?” and, “What rules are followed?” I then discuss what values are reflected in the breaking and following of rules.

### **5.1.1 Where Privacy and Security are Not Located**

There were numerous breakdowns where what would be categorized as rule breaking or a lack of rules in relation to security and privacy was observed or discussed. These breakdowns represent activities where conflicting objectives resulted in rules not being followed.

The breakdowns also demonstrated places where rules had not yet been instantiated in the socio-technical system. When rules are broken or uninstantiated this can mean that client information is provided without permission and that client privacy has not been respected.

#### **5.1.1.1 Rules in Conflict**

Rules, whether external or internal, are policies that are supposed to regulate access and management of client information. The breakdowns that occurred because of conflicting rules are ones where rules have been established to designate places in the socio-technical system where harm can be done (e.g., a privacy breach). Yet, because of local circumstances and local policies, there were breakdowns that demonstrated participants not following rules.

What is important is to understand what constitutes as privacy and security in this space and what does not. Rules were not followed because security and privacy were not

embodied into these local and individual practices, or because the rules are in conflict with each other.

The first example, and perhaps most canonical, of conflicting rules are the instances when HIPAA was not followed yet local and individual policies were. HIPAA is a US regulation that stipulates how offices can store and share electronic patient information. With HIPAA perceived as an external set of rules, when local circumstances and policies dictated different needs, HIPAA was ignored.

This conflict is demonstrated in the breakdowns involving disclosing patient information. For example, there was a breakdown where the receptionist did not see the harm in providing a husband with the location of his wife. There was another breakdown when the director did not see the harm in leaving files on the top of her filing cabinets. Last, there was a breakdown receptionist did not see the harm in shouting identifying client information to a room full of people. In each of these breakdowns, what was valued and what was enacted was helping a patient, finding files quickly, and correctly identifying the patient.

The threat was not present in the actions that people were taking. Additionally, the objective of the task was in conflict with HIPAA, and thus HIPAA was ignored.

There were two additional breakdowns where HIPAA was raised by someone in the center as a reason for people to behave in a secure manner. In these two breakdowns two separate nurses at separate locations raised their concerns. Yet, these concerns were discarded, even denigrated. One of the nurses was even called, "Little Miss HIPAA," in a style that was similar to calling someone a tattletale in grade school. In calling someone "Little Miss HIPAA," the name-calling reinforces an us-against-them mentality when it comes to following rules. It implicitly states that this is the way that we do things 'round these parts, are you with us or against us? Or, to say this another way, it enforces that local policy trumps national regulations (i.e., HIPAA).

While there is no literal line drawn in the sand, the delineation between local policies is made clear to those who work in these centers. This is because local policies reflect local needs. For example, when a family member calls the doctor about a patient the doctor recognizes the local needs: to present quick solutions to patient care problems. Yet, this is in direct discordance with the HIPAA rule of obtaining consent from all patients before discussing health information.

This HIPAA rule is created to protect a client's privacy, but in protecting the client's privacy the client may not gain adequate care. What results is the doctor being placed in a conundrum between his sworn oath to "do no harm" for this one patient at this one time against HIPAA which protects the generic patient's privacy. From the data in this dissertation, the local circumstance trumps the generic case.

There were also breakdowns in childcare centers where local policy in regards to a child's information were in conflict with state mandated policies. For example, there were

breakdowns where a director was observed to be filling in information on a form for only parents, a licensor was observed to not issue a citation when she saw that client information was not being managed correctly or securely, and teachers disclosed the name of biters in their classrooms to concerned parents. In these breakdowns, the staff were aware of the rules, yet because of the local needs these rules are obfuscated: the director believes that the child was picked up by her parents and she is safe today; the licensor believes that the files will be put securely away at a later date; and, the teacher believes that by divulging the name of the child the parents will have more success in rectifying their problems.

The value is not in the rule, but understanding the particular circumstances that necessitate the work to be done. These examples demonstrate that when local need conflicts with privacy policy in childcare centers, the people involved will evaluate the tension that exists to determine what is the proper course of action.

In a last example from childcare centers, the negotiation between local practice and rules is perhaps most represented in Figure 18. In this artifact the director has created a one-page condensed list of what three pages of licensing regulations actually translate to mean for her center. The assistant director goes from room to room and uses her list, thus instantiating the recognized negotiation between her and her childcare center licensor.

There are times, though, when even local or adopted rules can be broken based on the context. For example, a nurse was observed to call her friend with test results even though this is against the center's policy. In this case, the nurse breaks the local rule in order to better establish her relationship with her patient and friend.

Based on what was observed and discussed by clients, speculations can be made about why local circumstances take precedence in relation to security and privacy. The first is that access to client information is limited. When shouting the patient's name, this is to a limited set of people who are in the waiting room; when faxing over an x-ray to a doctor for a consultation, it is a single x-ray and not the whole client history; when providing the location of the patient to the spouse, it is to one person.

The circumstance is not just local, but it is reciprocal to the scope of the information. In this sense, a boundary is established between providing access to all client information, to what is necessary for that circumstance.

The second reason why local circumstances take precedence is a lack of accountability. There is no audit trail to show that this information has been leaked or a rule has been broken; there is no exact accounting that shows on November 2<sup>nd</sup> Nurse-N disclosed the patient's name and address in the waiting room. This lack of accounting decreases the impetus to follow policies since they lack enforcement. For example, after the nurse called her friend, she placed the file in the to-be-shelved pile instead of the need-doctor's-attention pile. This means that no one in the office was the wiser breach in policy. The lack of accountability means that in breakdowns where there are conflicting rule, not

following policy can become invisible work, and thus leads to a lack of adoption of standards like HIPAA.

The last reason why local circumstances take precedence is these situations couch privacy and security in the intimate trusting relationships that exist between the actors. While this will be discussed further in the section on Communities of Security, the relationships between people in these offices embody and instantiate trust. It is the relationship between the husband and wife, and wife-as-patient and the director that is being evaluated (correctly or not). Similarly, it is the relationship between the two doctors that is being leveraged; the doctor trusts that the consulting doctor is not going to run to the black market and sell the client's x-ray. By locating the value of security and privacy within the intimate relationships instead of within policy, it detracts from the value placed on policies.

Together, the limited scope of information, the lack of accountability, and the relationships surrounding the conflicting rules all enable security and privacy to be obfuscated in the interest of conflicting local needs.

All of these breakdowns highlight how rules, like HIPAA, are enforced through their adoption. Without that adoption, rules can be ignored. For software, this creates a strange design decision to either support the local policies, or supporting how HIPAA says that information should be managed. If the system does not support the work that people want to do, it will not be used; however, if it does not embody policies like HIPAA the system could be liable for patient information disclosure.

#### 5.1.1.2 Uninstantiated Rules

There were breakdowns where an adopted and explicit rule had not yet been instantiated. Rather than halt all work and hold a town hall meeting with all relevant stakeholders, on the fly policies and rules were created to meet the needs of the activities. The problem arises when these policies do not respect the privacy and security of the client's information or, when the policy is made more public so that other stakeholders can report their dissatisfaction.

The first and most representative example is in the teacher's undisclosed use of a child's pictures on Facebook. The lack of a childcare center policy stipulating if a child's picture could and could not be used on the internet had not been created. This lack of policy led to teachers using pictures showing them with the classroom's children on their Facebook profiles. The breakdown arose when teachers at the center "friended" some parents and the parents reacted poorly to seeing the picture of their child on such a public forum.

What resulted is the child's picture being taken down, the parent being "unfriended," and a new policy about using children's pictures on social networking websites. However, before a new rule could be created, the uninstantiated policy resulted in actions that represented local needs and not necessarily the best decision when it comes to the security and privacy of client information.

There were other examples where a rule was observed to be uninstantiated and resulted in questionable privacy practices. These include the lack of an information access audit trail, staff sharing passwords and log-in information, the general lack of password use even in places that had them, the fact that client files have an indeterminate life time, and the relative open access to client information. In each of these breakdowns, there is not a policy that can be enforced to make people use passwords, to make files be locked up every second that they are not being used, and to make an audit trail exists.

This means that people do what is easiest. They share and shout passwords, they leave client information on counter tops (e.g., x-rays, transcripts, immunization records), and they have little idea of who accessed an electronic file.

Malevolence is not present in these actions, but the problem is that managing privacy and security is not easily embodied into the everyday actions of these locations. Additionally, there has not been a security threat that has caused the staff to recognize the value of passwords or locking files nor the liability of not locking.

### **5.1.2 Where Privacy and Security are Located**

Given the previous discussion on where privacy and security are not located, this section pushes back on the assumption that privacy and security do not exist. Instead it discusses the places where security and privacy were observed to exist.

#### **5.1.2.1 Security and Privacy are Local**

The first realization of researchers when engaged with childcare centers and physicians offices is the sheer messiness of what might be thought of as mundane work (Miller et al. 2001). What looks from the outside to be a normal daily routine (children enter, stay for the day, and leave with parents; patient enters, issues are attended to, patient leaves; patient enters, meets with nurse and doctor, pays for service, leaves) is actually “improvised choreography” (Whalen et al. 2002).

Childcare centers and physicians’ offices are constantly evaluating, re-evaluating, modifying, and applying policies to reflect the nuanced work that needs to be done. No one client’s needs are the same, nor is their response the same, nor is how their documentation handled going to be the same. This means that the needs for documenting and managing client information need to reflect the improvisation of policy.

The question becomes how does all the improvisation affect privacy practices? O’Conaill and Frolich found that when people are interrupted in their work, which serves as one kind of need for improvisation, 41% of the time they do not return to the original task (O’Conaill et al. 1995). Thus, if a director is disturbed while accessing a child’s file, or updating information about a child, this task may not be completed for some time, leaving information that is sensitive in an open working environment or a file lacking critical information.

But when many practices are implemented on the fly, so too may privacy practices be created and utilized. For instance, the director of Child-P01, in moving into a new

location, had the child's files strewn across the floor to use and file. She made a special practice of closing and locking the door to her office to keep the files secure. For security, where pre-defined rules and standards of behavior are the common tools for enacting privacy needs, the dynamic nature of child and patient work is ill suited.

Therefore the security and privacy is embodied into the local situations with nuanced needs. It is when policies and systems do not support or represent local needs that breakdowns occur. For instance, in the observations of both patients and health care personnel disregarding the important privacy policy, there is an implicit recognition that the privacy policy does not actually represent how the client's information will be managed. Similarly, one childcare center director reported that she had to remove the signature page from the back of the childcare center's handbook during enrollment because otherwise parents would not sign and return it.

These breakdowns are occurring because both parties in the privacy agreement acknowledge in their dismissal of the privacy policy that these are the official policies, but not the real ones (i.e., why the nurse tells the patient that she can wallpaper her bathroom with it).

In essence, the privacy policy does a disservice to the client-center relationship. That is, the ostensible purposes of the handbook and privacy policy are to locate policy in official contexts. Yet participants in the system may operate on a more relational understanding of where policy is located.

The handbook and the agreement may be considered fallbacks in case of trouble, but most of the everyday problems that arise will not be described. This is similar to Gee's observation of the several intermingled layers of "who's-doing-whats" on the instructions and warning on the back of an aspirin bottle (Gee 2005). Instead of the handbook and privacy policy reflecting the real daily practices, official ones are used to report best practices. This means that clients have little official knowledge that anyone in the center can access their information, that pharmacology representatives can receive and read copies of their file, and that passwords are not being used.

#### 5.1.2.2 Security and Privacy are Individual

Security and privacy are also embodied into individual needs and beliefs. Beyond local, individuals reflected that they have ways of interacting with client data and beliefs about how to interact with client data that was unique. These individual needs and beliefs are important because they demonstrate the dangers of one-system-fits-all users model.

In the first example, staff at childcare centers and physicians' offices explained their incorrect beliefs about security and privacy. Perhaps the most salient of these breakdowns is when the childcare center licensor told the observer that she does not use passwords because she believes that they are essentially useless against faceless hackers. In this instance, the problem goes beyond the lack of rules, or a conflict with local policy. Her incorrect beliefs about how security works are directly translated into an insecure computer that contains sensitive child information.

Incorrect beliefs about how technology works in reference to security and privacy demonstrate the dangers of not using policies that can be understood and adopted at the individual level. Requiring childcare center licensors to use a password on their laptops is not enough; the threat is not salient.

In the second and third examples, the EMR system was reported to not support the needs of the doctors in the office, either by not providing the ability to audit other people's work or by providing inadequate fields to support entering client information. These problems result in client information being duplicated, stored in additional forms, stored in additional unsecure locations, and more people accessing and annotating client information. A recent post from Dr. Ofri, a columnist for the New York Times, explained this problem more fully:

Electronic medical records promise efficiency, safety and productivity in the switch from paper to computer. But there are glitches... After our physical exam, I sit down to write a detailed evaluation... As I type away, I feel like I'm doing the right thing, explicating my clinical reasoning rather than just plugging numbers into a formula. I'm midway into a sentence about kidney function when the computer abruptly halts... It turns out that in our electronic medical record system there is a 1,000-character maximum in the 'assessment' field... I nip and tuck my descriptions of his diabetes, his hypertension, his aortic valve stenosis, trying to placate the demands of our nit-picky computer system. Nevertheless, I am still unable to fit a complete assessment into the box (Ofri 2010).

Dr. Ofri, in explaining her problems with her EMR system, demonstrates how her desire to enter relevant (and sensitive) information about her patient is being limited. Her individual preferences for reporting client information results in what she deems as an incomplete record. This incomplete record demonstrates not only a possible safety problem for relaying information, but also a problem in reference to reflecting individual needs in electronic systems.

Limiting care workers to systems that do not support the work they want to do resulted in documentation that does not reflect the care that was being provided. In reference to security and privacy, this leads to fragmentation.

More broadly, by not supporting individual needs, the users circumvented external and local policies for their individual needs.

### 5.1.2.3 Security and Privacy are Care

When push comes to shove, providing care for a patient was seen to come before providing privacy and security. Examples include when the childcare center teachers would disclose the names of the biters in their classrooms, or when the doctor provided information about his clients to concerned family members. However, when privacy and

care were not in conflict, privacy and security was seen as representations of care of the client.

One childcare center director talked about managing “little lives” in reference to not just managing the children in their daily lives, but also managing the children’s paperwork. The documentation and the management of that documentation are part of the care being provided to that child. Making sure that the child has up-to-date immunizations is important not only because it is mandated, but because the directors see it as their responsibility for children to be properly cared for.

Beyond paperwork, there were breakdowns where privately and securely managing a child’s information was part of the care. For instance, childcare center personnel are mandatory reports of child abuse. Yet, when it came to documenting the evidence of abuse, particular care was provided to keep the information discreet and private. This was done not only to prevent gossiping, but because, as one director explained, she wanted to protect the child in case they were wrong.

Similarly, a different childcare center director explained that there are specific instances when security and care are synonymous. These are in instances when the child is being fostered or when parents are battling over custody. In these cases, security of the child is translated not only into additional security for the child but also for the child’s information (e.g., special care to document who is picking up the child).

Similarly, physicians’ offices also embodied security and privacy into the care of their patients. There are three relevant examples. In the first breakdown a director reported keeping client information for so long because she wanted to be able to care for that patient again if they ever returned. In second breakdown, an office called a satellite office to pass along patient information that was relevant for care because the patient’s file would not arrive in time for the appointment. In a last breakdown, information about a client’s financial problems was kept private and disconnected from her medical record in order to respect her privacy.

These examples all demonstrate breakdowns where client care embodies security and privacy. This means that a client’s information and the management of that information cannot be separated from the care that people receive.

Difficulties occur when privacy and security are perceived to be in conflict with care. For design, this means understanding when the two are in conflict, and then mitigating or supporting the work that people need to do rather than the need for privacy. For instance, one of the largest concerns with work in security and privacy in health care is the question of what to do in an emergency situation where access to all information is necessary to treat the patient. The answer in this case is simple. The designer could provide open access in emergency situations, and in the more nuanced versions (such as a biter in the two-year-old room) provide information that is harder to access.

#### 5.1.2.4 Security and Privacy are Robustness of Information

Numerous breakdowns were related to the robustness of client information. Robustness of information is how up-to-date and complete the client's information is.

Breakdowns occurred because out-of-date information can result in a licensing violation for childcare centers and can result in harm for both patients and children. For instance, a missing phone number was critical in not being able to locate a child at a childcare center. For these reasons, a large part of the security of information was related to how robust it was.

Examples of efforts to keep information robust were demonstrated in cases where there was missing information to go into a client's file, when there was incorrect information in a patient's file, when patients were indeterminately missing or dead, when both childcare centers and physicians' offices had difficulties gathering new information from patients and parents, and when staff were determined to not document adequately about a child's progress.

In all of these examples, efforts were taken to rectify incorrect information about a client in an attempt to gather and gain knowledge about an objective truth. For instance, not documenting a child's progress adequately was a problem because it limited the conversation between parents and childcare center staff about the development of the child. Which, in turn, was reported by the childcare center director to be related to a parent's trust of the childcare center to care for the child. This, in turn, affected parents when providing information about their child. Thus, the original problem of not documenting enough about a child was one part in a continuing the feedback loop of determining some objective reality about the child's development.

#### 5.1.3 Summary

In this section I presented and discussed examples of how security and privacy are embodied. In the first section I discussed places where security breakdowns were encountered as representative of where security and privacy are not located. I then juxtaposed these examples with the practices that do embody security and privacy. Security and privacy were reported to be local and individual, and deeply part of the activities of caring for the client and making sure the information was robust.

In response to earlier questions about threat models and their relation to understanding security and privacy, this discussion demonstrates some of the problems with relying on only a threat model for understanding security and privacy for design. With a threat model there is not an easy way to account for instances where local and individual needs will come into conflict with policies. Additionally, it is hard to account for the small daily needs that influence the management of information. For example, the breakdown where the staff bothered a client repeatedly until they provide necessary information illustrates the issues surrounding social pressure and individual needs, but would be difficult to explain using a threat model.

Threats were not a relevant and represented factor for managing sensitive client information. Even in the discussion of nameless hackers was raised by the childcare center licensor, this nameless rascalion was not enough of a threat to influence how she was interacting with client information; the threat was not salient.

Instead, the factors that did affect the management of client information demonstrate that security and privacy are valued, but in methods that are not easily accounted for. Examples of these will be demonstrated in the following chapter.

## ***5.2 Communities of Security***

It has been one of the central tenants of the research on computer supported collaborative work that people do not act as individuals. Instead, people interact, react, and are mediated through the actions that they have with one another.

The interaction with computing systems is no different. Computers are used as tools to interact, react, and mediate actions with one another. However, when it comes to the design of secure systems, many have been designed for the individual rather than a community of people bound together in joint activity. For example, one person is given one password to work at their one computer; or, one file is associated with one client which has one unique ID.

Yet, as will be discussed in this section, this is not how the people of these centers account for their work. They view their work as one cog in the larger system of care. For example, a receptionist may retrieve a file for a nurse, and place it on the table. The nurse may scan the file, and then pass it onto the nurse who is seeing the patient. The new nurse may make annotations on the file when she sees the patient. The doctor, the office staff, and a nurse may make notes as the file moves from location to location. Later transcriptions of the patient's appointment may be added along with faxes in regards to prescriptions or referrals. Each of these additions could be reviewed and added to the patient's file by a different person at different times.

The location, number of accesses, and diversity of people who access the file is a microcosm for managing client information. Yet, the work gets done in such a way that the client's privacy is respected and the information is kept secure.

I define a *community of security* as the interactions and relationships that instantiate a community when in the co-constructed task of security and privacy. By focusing on a community of people, the concentration moves away from the individual to account for the larger task that is being accomplished. For example, this means that the macro-level task of care as it embodies security and privacy can be accounted for within by the mutually deterministic individual actions in the socio-technical system. In essence, the individual actions are less than the sum of their parts. Together when combined to examine the larger activity that is being represented in individual activities, the larger goal and need is apparent.

Within the realm of centers managing sensitive client information, a community of security is defined as those people who have interaction with a client's information by either providing, accessing, or managing the information in a secure and private way.

In the following sub-sections communities of security are used as a lens to evaluate the value of roles and relationships in regards to security and privacy.

### **5.2.1 The Value of Roles in Relation to Communities of Security**

Roles reflect the job that people are supposed to do. For example, in childcare centers there is the director, assistant director, receptionist, lead teacher, teacher, child, parent, licenser, and many others. In physicians' offices there is the director, office staff, receptionist, nurse, doctor, pharmacology representative, insurance representative, and many others. Each these roles reflect various job functions to be preformed. The receptionist, for instance, is to greet the patient; the director is to manage client information and external relationships. Based on roles there are assumptions about the kind of information that that person will need to access.

The use of roles has become an adaptation in security systems to restrict access to information. This adaptation is called "role-based authentication control." Instead a single user being accounted for and a unique policy made for them, a user is assigned a role. The role has pre-determined access to a system of information (Ferraiolo et al. 1992).

In childcare centers and physician's office, the official policy was that roles do exist. These roles represented restrictions to the client's information (Vega et al. 2009a; Vega et al. 2009b). For instance, office staff members were reportedly restricted to only have access to billing information. In childcare centers, teachers were reported to have restricted access to a child's file, and parents in two childcares centers were allowed to formally designate who could access their child's information. The official policy was that the roles people played in centers could be translated to who could access client information. However, what was observed was quite different from the official policy.

This is because the participants in this study did not view the work that they were doing as necessarily representing only those roles. What was observed was that people had to put on many different metaphorical hats to manage the busy and messy work involved in these centers.

Indeed, wearing many hats was required for the centers to function. Nurses were observed collating forms, doctors pulling patient files, directors rocking sick children, the assistant directors serving as cooks, and the cook serving as receptionist. Prior work demonstrated that even when looking at communication in a cardiac intensive care unit that eavesdropping by nurses, doctors, and other health care workers was critical in managing a patient's care and safety (Vuckovic et al. 2004).

This is important in reference to security. If the work that is required for the center to function cannot be located around the roles that people are given, than how is information to be kept private from different people? For instance, there was a breakdown when a

teacher attempted to access the files for the children in her room, an act that is restricted not just by the official local policy but also by the parents and the accreditation agency. However, what was revealed and duplicated again later, is that the teachers are provided access to that information even though it is against the policy.

The use of passwords, or the lack there of, and the open access to client information at both childcare centers and physicians' offices is perhaps the strongest example of the problem of assumed individuality in these centers. Staff shared passwords, shouted passwords, and many centers did not use them at all. When questioned why, one director explained it is because "<people in the office> can access anything. That's their job." It is the job of the people there to do the work, not for them to follow the exact role of their job.

This is more than the fact that research has found that when security gets in the way of a primary task security is ignored (Adams et al. 1999). This is a reflection about how people in the office represent and evaluate the work that they do. People in the office see that they do individual tasks, but they are only smaller sub-tasks within the larger task of patient care. This means that when there is a problem with care or there is a problem with security, it is a problem for the center and not just a problem for an individual person.

Examples of how the centers viewed their work were expressed in breakdowns. For example, in the breakdown where physicians' offices prepared for incorrect patient information, the goal was not to protect one patient or to protect and identify the one person who was doing the task incorrectly. The action was about protecting the center. This is similarly why the staff at centers were not overly concerned with knowing who had accessed or modified client information. The mere fact one person in the office had accessed or modified the client's information was representative of a need for anyone in the center to possibly access or modify the client's information.

The lack of a practical delineation of roles facilitated many important needs in the centers. It allowed the receptionist and the echocardiogram technician to catch fatal tests. It allowed for scanning and reviewing client information to be documented in client files. And, it allowed people in the center to stay current on the local and contextual needs of the business.

Without accounting for the variable nature of the roles that people can play, security will possibly hinder access to information that is relevant to the needs of the center, thus resulting in circumvention.

Yet, there were times when roles did play an important part in the management of sensitive client information. For example, the doctor desired to audit the work of the director, staff were observed to hide their personal information from one another, and sensitive information about clients was stored in particular locations that only one person knew about. Additionally, having knowledge of who had accessed a file last provided clues in being able to locate a missing patient's record.

These examples are highlighted to demonstrate that roles are not useless in the design of secure systems. Rather, role should represent the work that people officially do and then the work that they actually do.

The dynamic interplay of roles was most apparent in the delineation between those viewed as external and those who were viewed as internal to the center. People who were external were viewed as having restricted access such as Department of Social Services Representatives, Insurance Companies, and other centers.

In particular, clients were considered as external. As parties on either side of the divide, clients and directors have different goals, knowledge sets, and authorities that translate into asymmetric awareness, access, and control of the client's information. For instance, childcare centers and physicians' offices were observed to restrict access to clients their information. Directors also expressed a hesitation about what to write down and store in the client's file because of how it might be perceived by the client when reviewing it (resulting in filtering any information the client would actually be able to access).

The "us versus them" mentality that can sometimes arise when these external versus internal debates take place was summed up well by the licensing agent and with agreement from Child-P01: "Burnout rate is high in daycare, but it's not the children... it's the adults."

With the evidence presented in this dissertation, roles both represent what information people *should* be able to access, but also represent what information people *actually* are able to access. This is because, as supported by the work of Sinclair et al. (2007), roles are messy. For example, in a study of one business group of 3,000 people a third of them changed their roles within a three-month period. This translated to new information access, not releasing access to old and unused information, and an over-entitlement to information. In fact, Sinclair et al. were able to predict how long someone had been at the company based on the amount of access they had (Sinclair et al. 2007).

The question becomes how to use the power of roles in reference to security while also respecting the contextual needs that frequently do not fit the boundaries of that role. Possible solutions could include decaying access, location-based access, and other mechanisms that respect that roles are fluid.

### **5.2.2 The Value of Relationships in Security and Privacy**

An economic exchange model of privacy is often used to envision privacy-related situations. In this model, the user of a service makes a rational judgment about giving up some of their private information in order to gain a service. In the childcare center and physician's office context, we could characterize the tradeoff as a client being willing to provide sensitive information to enable care.

"Exchange" relationships such as those assumed the economic exchange relationship assume a localized tit-for-tat model of self-interest. These are common in the world of commerce. However, personal or familial relationships can usually be characterized as

“communal” and involve longer-term assessment of gains and losses. Many valuable characteristics of childcare centers, for example, depend on the maintenance of communal interests that prioritize the well being of the mutually-cared-for child (Clark 1984; Clark et al. 1985; Clark et al. 1989).

Furthermore, as Dourish and Anderson (2006) explain, even in less fraught circumstances, users in actual practice do not always behave in a rational economic manner. Users can hand over what would be thought of as very valuable information for very little pay back. But much of the information we are talking about has no market value unless you are famous (AssociatedPress 2009).

Ultimately, the economic exchange model is insufficient to describe the problems of security and privacy in these contexts, or the trade-off decisions for clients. It fundamentally fails to reflect the social nature of privacy: “Privacy is not simply a way that information is managed but how social relations are managed” (Dourish & Anderson 2006, pp. 327). By understanding how clients and center personnel see and value the sensitive information they are interacting with, a deeper understanding of their security practices can emerge.

Similar to the arguments in relation to privacy as a collective practice, privacy is more than how information is stored and managed, it is also about the social relations that create the privacy policies (Dourish et al. 2006). In the childcare center, parents generally create a sense that their child is safe. Then, this feeling of safety translates to feeling that their sensitive information is safe. For example, until stirred up by our questions, parents were in general happy to leave informational practices as the business of the childcare center, while the staff at childcare centers were happy to treat their practices as background to the main job of childcare center. This is because of the relationships that are intimately involved and mediate the management of client information.

A function of relationships is to hold people mutually accountable. In reference to security and privacy, what was demonstrated in the data was that the local relationships played an important role. For example, as discussed in a previous section, patients disregarded the privacy policy provided to them by their physician’s office.

One reason for this is because patients were relying on their relationship with their care provider to mediate in the management of their sensitive information; or, in other words, they trusted their care provider. The patient recognizes that they have little ability to regulate their information themselves given the current socio-technical system. They are therefore placed in a situation where they have to trust the physician’s office or forgo care.

However, the relationship between the patient and the physician’s office was demonstrated to be one of handing over information in order to provide care while possibly forgoing privacy. Patients were observed to provide additional information about their illnesses and medical history that were not accountable in the forms that were

to be filled out. This act demonstrates that knowledge about the patient's is co-constructed between the patient and the health care providers.

This co-creation of information is built by the intimate relationship between local people. In these situations, what was of concern was not the doctor's relationship with an insurance company (although this will be discussed later) or the patient's relationship with another care provider. What was valued was the one-to-one relationship that enabled information disclosure.

Information disclosure was the foundation to information management. After all, it is hard to manage information if no information is being provided. However, information disclosure necessitates trust, and trust necessitates relationships.

Another relationship that was reliant on trust for information disclosure was the one that exists between physicians. Doctors were found to communicate information to other doctors to acquire a quick off-the-cuff diagnosis about their patients. For instance, a dermatologist may send test results of a biopsy to another doctor for a quick analysis.

What is being demonstrated in this example is the role that trust plays in sharing sensitive information. Doctors trust they are going to securely manage a patient's information. Additionally, because the patient trusts their care provider, their trust is transitive to these secondary care providers. The backbone of the information sharing is the network of relationships that not only enable care, but also enable disclosure.

Intimate relationship that existed outside of the physician's office also demonstrated where policies would be broken to provide care. A nurse was observed to call her friend with test results even though this broke the local policy of doctors discussing test results with patients. What was valued was the relationship between the nurse and her friend. This relationship superseded the policy, resulting in information disclosure.

What is important to consider, though, is the effect that this action had. What occurred was a strengthening of the nurse's relationship with her friend, which only reinforced the mutual understanding of the importance of the care. Secondly, this demonstrates to the patient that privacy and security policies are not rigid and that official policies are negotiable in unique circumstances.

There were relationships that were not necessarily revealed to patients about who could access their information. For instance, patient information was shared with pharmacology representatives who were visiting the office. In one case, an entire patient's file was faxed to the pharmacologist's office to review the patient's insurance information and medical history.

The relationship between the pharmacology representative and the physician's office enables this degree of information sharing. The same pharmacology representatives were observed on numerous occasions visiting and bestowing gifts and food. One function of the repeated visits is to establish a relationship where the office staff feels secure in

sharing patient information if it is deemed in the best interest of the patients care. In the instance where the file was being faxed, the receptionist explained that this patient had the largest potential to receive benefits from the treatment. Therefore, providing the patient's information was seen as in the best interest of the patient's care, rather than as a privacy violation of the patient's information.

Physicians' offices were not the only locations where relationships functioned as the backbone for information disclosure. Relationships and trust were also present in childcare centers.

The relationship between the childcare center staff and the parents is particularly representative of importance of relationships. When parents were discussing how they trusted their childcare center, the participants cited relationships as integral. For instance, for the mother who lived an hour from her childcare center, what she reported to trust was not her childcare center, but her family members who lived close to the childcare center. Similarly, other parents reported that they trusted the childcare center director to properly manage the child's information. What parents did not trust was other people in the center (i.e., the people who they did not know). The relationships between the parents and specific people in the center facilitated the parents sharing information and the care of their child.

The trust in the childcare center director is particularly interesting because of her expertise. Childcare center directors have more access to and responsibility for the manila file than do parents (and especially because they manage dozens if not hundreds of files that reflect diverse circumstances), there exists a gap in expertise; directors are much more familiar about what is in the file, how long it is kept, which laws govern the file contents, etc.

The directors at Child-P01 and Child-P04 both explained almost completely the contents of the child's file from memory. In one incident the director at Child-P01 even spouted out the color of the paper that each of five forms is printed on, what the title of the form is, which information is on it, and what the information is used for. This means that the director becomes an expert at managing these files. She knows the laws that require the information to be collected and the timeliness with which they have to be updated (e.g. for monthly or yearly immunizations). And, she helps remind parents to get the required immunizations for their children.

The director therefore becomes highly knowledgeable about information management because of the number and variety (e.g., some children are foster children, have custody problems, special health or education needs, etc.) of cases she handles. It is through the expression of this expertise that parents come to rely on the childcare center director. This relationship is then valued and trusted, which thereby influences how parents disclose and rely on childcare center directors. For example, after the breakdown where the teachers posted pictures of children on Facebook, it was the director who talked with the parents and addressed their concerns instead of the teachers. It is the director's

relationship with the parents that is valued not just in terms of business, but in continuing to ground the relationship between parents and the childcare center.

However, the relationship with teachers is also important. After all, it is the teacher who the parents are entrusting their child to each day and not the director. While it is important to reflect that many parents said that they would not feel comfortable with their child's teachers having access to their child's information, teachers were relied upon to be primary documenters of daily information about the child. This daily documentation was valued to such a degree that when one teacher was deemed as not documenting adequately was removed from her job.

Relationships breed interdependence. For instance, because an interaction is repeated without any negative consequences (or with positive consequences) it is repeated. The nurse who always knows where to find a patient's file is consistently called upon to locate patient files. Or, because the director provides the pharmacology representative with the patient's information, the pharmacology representative continues to provide food to the staff.

Relationships also breed reciprocity. For instance, because the receptionist helps a nurse by rescheduling a grouchy client, the nurse later helps her re-file patient records. And, because the office staff helps the receptionist during a busy time of the day, she later spends time educating the nurse about erectile dysfunction in order for the other ladies at the office to stop teasing her.

### **5.2.3 Summary**

In offices that have electronic systems at least 50% of the communication was still face-to-face (Vuckovic et al. 2004). This is because communication serves a very important function. It creates a collective awareness of the work that is being engaged in and re-affirms relationships that foster the co-construction of information.

Problems occur in relation to security and privacy when there is not a proper understanding of the importance of relationships and roles. Roles and relationships are powerful factors for accounting for information sharing. For example, the role of the director can function as a gatekeeper (Vega et al. 2009a; Vega et al. 2009b) and the relationship that the director has with various people in the office can affect who can access what information in different contexts.

However, electronic systems do not account for information management in the same way as social systems (Flechais et al. 2005; Dourish et al. 2006). People are assigned roles with certain access that does not account for their work or contextual needs (Sinclair et al. 2007); nor are relationships, such as the nurse-to-patient versus doctor-to-patient relationship, accounted for in electronic systems.

In particular, patients and parents are viewed as external and as outsiders who have little access to their own information. The growing patient agency in electronic record systems is not properly reflecting how the current socio-technical system accounts for the parent

and patient role. This creates a system that compromises the center's privacy and information management practices.

### **5.3 Zones of Ambiguity**

Part of the value of rules and policies are the boundaries that they indicate: forms must be returned by this date; patient files are kept under the cabinet until transcriptions are approved; teachers should not access a child's information; and, allergy information must be displayed in classrooms and kitchens. Policies, in essence, represent the marked end of information management. They articulate how things are to be done and how privacy and security are to be accounted for.

However, for every marked end there is also an unmarked end. There will be places in the socio-technical system where rules do not exist. This can result in ambiguity.

These unmarked places are one of compromise and negotiation; they are what I have called *zone of ambiguity*. Specifically, in the work of security in childcare centers and physicians' offices, a zone of ambiguity is where current behavioral practices allow fundamentally contradictory concerns to exist in tacit compromise with one another. Zones of ambiguity are those components of the practices that might have to be resolved with the addition or enforcement of a more official protocol upon the introduction of computerized information handling mechanisms.

The challenge of designing computational systems is that making these concerns explicit risks failure to find similar tenable compromises. Zones of ambiguity therefore identify loci for (future) design and innovation focus in the creation of secure, private systems of information management.

In this section I examine the data from the previous chapter in reference to ambiguities that exist within the current socio-technical system. I then present a discussion about how these ambiguities are responding to changing client agency in electronic record systems.

#### **5.3.1 Ambiguities**

##### **5.3.1.1 Content is Ambiguous**

There are numerous policies that exist to indicate the content of a client's file. For instance, childcare center directors provide parents with packets of information to be filled out before enrolling a child. Similarly, new patients are provided forms that must be filled out prior to being seen by the doctor. There is additionally routine information that is collected (e.g., blood pressure), along with annual information that is collected (e.g., immunization report). There is even state mandated information that is to be collected (e.g., privacy policy agreement, copy of custody agreement).

These examples demonstrate demarcations of where the content of information is to be collected: the blood pressure is 120/70, the child received a hepatitis B shot, the privacy policy is signed, and only dad can pick up the child on Fridays.

However, the content of client files was actually more ambiguous. For example, both the staff at childcare centers and physicians' offices reported instances where they were hesitant to document information about a client. Nurses and directors were particularly hesitant to document problems that were relevant for them providing care to the patient, but could later cause difficulties when viewed by someone external to the center.

Given that patient files can be subpoenaed and that HIPAA stipulates that a client can access their file at any time, participants reported fears about documenting problems such as a "difficult" (read: obnoxious) patient or for a receptionist to make notes about a patient appearing to be "confused" (read: she thinks they might be early onset Alzheimer's).

In essence, what is occurring in these situations is a contention between liability and care that can affect the content of the file. What results is ambiguity over what actually constitutes as the patient's file. Is the patient's file all of the notes in the margins, the layers post-it notes, the billing information, and the extra sensitive information about family troubles? Or, is it simply the transcriptions from appointments and the forms that patients filled out?

The decentralization, distribution, and layering of patient information creates a nexus of sensitive information that is difficult to delineate what is a patient's file and what is not. This allows for physicians' offices to have varying local policies when patients ask for a copy of their medical record or when the files are subpoenaed. What constitutes as a patient's file in one location may not be the same in another.

This ambiguity facilitates the balance between liability and care, by allowing the physician's office to create a local definition of a patient's file that reflects the official policy and contains the official content; while, at the same time, it allows the physician's office to maintain information that that helps them manage the care for their patient.

In the last but perhaps most serious example from physicians' offices, staff at Med-P15 discovered that one of their patients was a sexual offender (and another was being charged with being a sexual offender). The question was what to do with this information? The staff at the office had to communally rectify having this information about their patients with the fact that they are charged with providing medical care.

In this breakdown a proper policy and protocol had not been established for documenting a patient as a sexual offender, yet this information was now known. What resulted is everyone in the office having communal knowledge of the patients, but no physical record left in the patient's "official" file.

Childcare centers were also found to have ambiguity over the content of a child's files, but for different reasons. The simplest example is the breakdown where the people at the childcare center knew that the person who is listed as "dad" in the child's file is not really the child's father. These cases reflect times where the official policy, e.g. the father's

name must be listed on the forms for the child to be enrolled, is influenced by the parent's need for privacy.

Similarly, parents discussed times when they did not provide their child's social security number to their childcare center because they did not want the childcare center to have this information. Parents (and two patients) found ways of providing either incorrect information guised as correct information, or found other methods to not provide the information (e.g., continually reporting that the social security care was left at home).

The tension that is reflected in these breakdowns is one between a client's privacy and the center's need for accurate information. What results is an unofficial understanding between the center staff about the content of the file. This unofficial understanding is one that is not documented in the client's file but in the social knowledge of the office staff.

#### 5.3.1.2 Accountability is Ambiguous

As discussed in the second section on Communities of Security, the work that people do in childcare centers and physicians' offices are not merely individual actions but represent a larger task of providing communal care. This model of work, one that is shared and distributed, is problematic for security and privacy that accounts for security and privacy on a one-to-one basis. What results is the communal work practices not being reflected in the security and privacy policies provided in handbooks and formalized into software.

For instance, participants in both childcare centers and physicians' offices were observed to share logins, rarely use passwords, share workstations, and leave their workstation open. Additionally, participants did not have individual accounts. This meant that it was relatively impossible for people to audit each other's work.

These facts again demonstrate issues in relation client privacy. Each of these alone would be categorized as a security liability for the management of client information, and together demonstrate a clear misalignment of security needs versus security actions.

These low-tech security risks are listed by Kroll's Fraud Solutions division as the second most likely method implicated in the leaking and unauthorized access of patient information for 2011 (Merrill 2011).

What is important to recognize is the ambiguity represented in these breakdowns. The office staff, at times, does not desire to have accountability for the work that they do. The fact that the doctor pulls patient records or that the cook serves as a receptionist is not accounted for because it reflects the very messiness of the work that is occurring in these locations. The action of one, in a sense, is the action of all in the communities' goals.

Capturing discrete interactions with a client's file is not the goal of the task, and thus it is left ambiguous to represent the work of many. This ambiguity, however, reflects the tension between articulation of work and shared responsibility.

The research on articulation work argues for accounting or the work of people. However, this is directly in conflict with shared responsibility.

The data presented in this dissertation argues instead that people do not desire to have their work articulated, in part, because articulation reflects individuality. Small communities, while comprised of individuals, do not necessarily reflect on their work in this manner.

Awareness and a shared understanding of the flow of information are instead socialized, which allows for negotiation of what actually occurred. For instance, when a file is missing, it can be attributed to the person who normally misfiles patient records, but it is left not articulated; who created that mistake does not matter.

Articulation work seeks to support users through formalized accounting of practice. What is important and valuable is the recognition that the people in this study had the tools to do articulation work. However, they did not use these tools. They did not use them because they did not have the desire.

### 5.3.1.3 Information Management is Ambiguous

Not one of the interviewed parents knew how their information was stored and maintained. Parent-P10 said, “I would assume those are in a filing cabinet in there, but I don't know if it is locked or not.”

Parents have a set of concerns that are real. They must be satisfied that their family's “real” safety and wellbeing is protected. Safety includes both immediate physical and long-term issues. Currently, they are reassured by the continuity between privacy and security practices and their relative invisibility. The zone of ambiguity protects them from having to think too deeply about the implications and interdependencies of information and precisely how the childcare center operates. For instance, parents were found to have little knowledge of who could access their child's file or how long a child's information remains stored at the childcare center.

There were similar practices at physicians' offices with patient information residing in physicians' offices decades after the patient has last been seen and generations after physician's had stopped practicing. This problem goes beyond the long established practice of physicians' storing patient information, and the uses for this information.

Relevant examples include locating the real identity of Little Albert from infamous behavioral psychology experiment (Beck et al. 2009).

This problem is about the values that are ascribed to this practice of storing information (as a way to manage patient information) that are then in contradiction to the values of security and privacy. To manage this contradiction the practice of how long files are actually stored is obfuscated and left purposefully ambiguous.

The ambiguity allows for the physicians' offices to continue storing patient files without patients having to consider the implications for their personal information existing indefinitely.

Childcare centers and physicians' offices do in fact have considerable power over the information in a day-to-day way. However, by-and-large, there is no external economic incentive for them to abuse the information system.

Yet, the client's power in this situation is very limited. It consists of refraining from applying or leaving if information problems become too difficult. This means that between the choice of learning more about the questionable security practices of the centers, clients allow for ambiguity over how their information is managed to exist.

Additionally, given the client's lack of knowledge about how their information is being managed, the client has little knowledge of what actually is actually in their file. This allows for the center to create the façade of centralizing and securely managing client information, while still being able to do the work that is necessary for the business. The ambiguity allows for the client to continue to visit the center, by recognizing that the official policy does not actually reflect the real practices.

#### 5.3.1.4 Visibility is Ambiguous

Digital and physical worlds have completely different mechanisms for security management. The physical world allows for security to be managed with such intuitive mechanisms as visible, spatial, verbal, and social accessibility. There are certainly technologies that play a role in this, but their functional qualities are often incredibly intuitive (e.g., a manila folder).

Many security mechanisms are so intuitive that they are actually created by the users themselves (e.g., office spatial layout, hiding sensitive information at the back of a file folder, information obfuscation, etc.). These mechanisms draw on basic principles that are physically and socially intuited from a young age without formal education.

This is not the case in the digital realm, where underlying security mechanisms are extremely difficult to grasp without formal education (Whitten et al. 1999). Even the location of information with respect to client and server, the basic spatial landscape of the internet, cannot be understood by many computer users (Pettersson et al. 2005). Without understanding the basic mechanisms of digital security, simply using the security features without undermining them is difficult, and appropriation is rare if not impossible (due to either programmatic constraints or lack of education/comfort).

Dourish et al. came to a similar conclusion in their own paper: the "visibility of system behavior on their terms, or the lack of it, was often a reason that people understood whether something was secure or failed to realize whether something was protected" (Dourish et al., 2004).

The suggestion offered by Dourish et al. is to make security technologies “highly visible.” Another approach is to educate users about the underlying technology’s vulnerabilities (Sheng et al., 2007). Without either making the underlying technology more intuitive or providing accurate metaphors of their functionality, it seems that education is a requirement for improved security. In deed, that visibility is what allows for education of what security threats really are.

The digital-physical security mechanism divide renders users less able to make informed security decisions and leads to a sort of defeatism that is not seen as readily when discussing the physical world (Dourish et al., 2004). For example, the licensing agent observed at Child-P01’s facility observed: “If somebody really wants on [my computer] they're gonna be smart enough to get on it, whether I have a nice long 12-letter multi-digit pass code or not...” The licensing agent goes on to suggest that the childcare center information stored on her computer is not valuable and that even if a hacker did break into it, she would not be able to access the information because the applications that it is stored in are so hard to navigate. Finally, she states: “I don't do online banking, I don't trust any of that, I mean I just don't, I don't pay bills online, I don't do any of that because I don't trust that someone can't just come right in and scoop it up.”

This is the testimony from just one person in the childcare center information management structure, but this one account suggests a number of important possible issues for usable security: that users do not understand the enemy and, the value of the data that they are overseeing, are intimidated by the thought of having information that they do find to be sensitive on the web.

With regard to not knowing the enemy in a digital environment, this user seems to underestimate the skills of an information perpetrator (doubting that she can understand or circumvent obscure interfaces). Other possible misunderstandings are how a perpetrator might “get in” to the system (not spatially, as in through the front door of the childcare center), how she might intercept data (not audibly, by literally overhearing a conversation), how she can be detected (not visibly, as in sitting down at the computer to find data), and how she might be dissuaded from stealing sensitive information (not socially, through social constructions of where one belongs, because there’s little in the way of a society that can find and report the perpetrator).

Not only may the user be blind to these characteristics of a digital perpetrator (which are often fairly clear in the case of the physical perpetrator), but also, the user must learn a completely new way of understanding the digital perpetrator (e.g., the user must learn perpetrators need not be visible even when they are in the same “space” that she is).

The user also may not understand, as the licensing agent did not, the value of the information that they are in ownership of. The licensor’s computer contained, at a minimum, the names and contact information for parents along with social security numbers. While this is not the valuable bank account information that she is unwilling to put online, she fails to recognize that this information is important for identity theft, or

for spamming companies, and more. This lack of understanding of what might motivate the perpetrator is a continuation of the lack of understanding of the perpetrator's means.

The perpetrator is not visible, thus the center's ability to detect and understand the threats to the information are obfuscated away from the management of the client's information. For example, one physician's office had no knowledge that her computer system was not backing up the client's files daily. When the computer system additionally crashed, the office lost weeks worth of client's data and additionally spent time re-entering client information from the paper records. The activity of security backing-up client data was invisible to the work that the staff members were doing.

However, by blindly relying on the computer system to make adequate and useful backups of the client's files, the center is relying on the ambiguity of the visibility to result favorably. After all, someone at the office could have checked on the back-ups weekly to make sure that they were not corrupt.

Last, the current socio-technical system does not afford visibility of client's information to the client. While patients have a mandated right to their information, parents do not. Additionally, what is actually revealed to the patient was different from all of the information that is stored about a client. Clients were not notified when their information was missing, and not notified if and when people accessed their information.

#### 5.3.1.5 Client is Ambiguous

When does a client become a client? When does a client stop being a client? Breakdowns occurred because of ambiguity over what qualifies as a client.

The qualification of a client is important. It signifies the point where the center is held accountable for the management of the client's care and information. Yet, as was observed, the demarcations of what is and is not a client were ambiguous.

When a client first enrolls in the childcare center or when the patient first joins the physician's office, there is a packet of information that the client has to fill out in order to be considered a client. However, information is actually collected about a client prior to enrollment. For instance, childcare centers in this study had extensive waitlist systems that collected the age, name, date of birth, and contact information for many of the children in the surrounding area. One childcare center boasted having a four-year waitlist. Also in physicians' offices there were times at both Med-P15 and Med-P17 where the doctor attended to the care of the patient without the patient having filled out the enrollment packet of information.

Additionally, the office staff members were observed to spend time trying to contact and *post hoc* collect necessary information in order for the patient to be considered a client. There were even instances where the patient had been seen, but the client record had not been made.

The ambiguity over when a client starts to be a client means that the information that is stored about them is nebulous. To the patient, they start being a client when they are first seen by the center. However, knowledge about up-coming clients is important for the centers to managing their client load and for other purposes such as communicating with insurance companies and complying with VDSS requirements.

There were also breakdowns at Med-P15 where unofficial files were kept on friends of the doctors in order to manage care for the friend. These files were qualitatively different from the files of clients. The first and perhaps most important qualifier was that there was no billing information for the friend. The friend also was not required to fill out any official paper work such as family history or privacy policy.

How the information was managed for friends of the doctor was equal. The friend still had their appointments transcribed, the file was stored with the other files, and nurses were charged with answering questions for friends if the doctor was not available. Is this friend, in fact, a client?

Similarly, there was ambiguity over when a client stops being a client. Client information was observed to exist indefinitely for both childcare centers and physicians' offices. One reason provided was because the office never knew when the client might return and need care. However, many centers kept a client's file long after the client (and even the doctor) was deceased.

### **5.3.2 Client Agency & Ambiguity**

Many of the ambiguities in the previous section are reflections on the current socio-technical system where clients have little ability, even if they wanted to, to manage their own information. For example, clients were observed to try and provide additional information to the centers in order to take a larger role in the co-construction of information about their child and health. Additionally, patients were observed to call physicians' offices when information about their medical procedures was not clear.

It is important to understand how the rapidly changing technology environment can influence the centers that were studied and the relationships that they have with their clients. The landscape for managing child and patient information is shifting as electronic records and technology is moving into childcare centers and physicians' offices (Berner et al. 2005; Zhou et al. 2009; 2010d; Meyer 2010). Televised commercials depict doctors with handheld devices that can do on-the-spot sonic imagery and teachers video conferencing with classrooms across the world. With this proposed increase in technology adoption, I predict that there will be additional changes with regards to user agency for privacy and security, particularly within the health care realm.

This change is demonstrated in two examples. First, physicians are starting to employ scribes to annotate their dictations and master the "complex electronic medical record systems" (Meyer 2010). These new staff members are being added to the physician's office, thus creating an additional layer between the doctor and their annotation of sensitive information. In a second example, HIPAA stipulates that patients have the right

to not only see their information, but also to correct any misinformation. With the increased use in electronic medical records, this responsibility, which was nebulous before hand, may become clearer as patients have an increased (required) ability to see their own information.

The question remains though, who do patients contact about updating the information? The scribe? The electronic record support staff? Questions like these raise problems not only about allowing patients to protect their privacy, but about understanding how increasing the patient's agency in the health care relationship with technology is going to change community norms surrounding sensitive information management.

Recent surveys and technology developments have shown that patients not only want to see their personal sensitive information, but that 40% of those surveyed reported that they would pay for a service that would send real-time medical information to their doctors (2010d).

Indeed, with increase in patient agency into the realm of electronic health records, so also is there an increase in the electronic information out there. This includes information being sent from blue-tooth enabled pillboxes, stethoscopes, and even research into how to how to encapsulate a transmitter into medicine.

The same increase in technology adoption was observed in childcare centers: parents want text messages about childcare center closings and childcare center directors expressed worry about their online presence. With the increase in information being transmitted by devices and through additional communication channels so also exists the need to understand, at a basic level, how all this information is being amalgamated, and at a higher level how all this information is being made secure.

Another important distinction is that in centers, security is not just about preventing break-ins, but is also wrapped up in the willing disclosure of information and in the accidental undermining of security systems (e.g., leaving the door unlocked, teaching children to push the green button, etc.). Sometimes it may be necessary to discuss precisely who bit whom or when a patient is being obnoxious.

#### **5.4 Summary**

In this chapter, we have explored the halls of childcare centers and physicians' offices. I presented what they do, how they do it, and most importantly, why. We have found that the dynamic, unpredictable nature of day-to-day affairs renders ambiguity a requirement. Ideal information practices are thus foiled by unexpected events and the resulting situated security measures hinge on various local policies.

The dynamics between client and provider is such that various asymmetries of information awareness, access, and control exist and require the embodiment of security and privacy into everyday behaviors. We have also seen how these findings may speak to the impending movement of documents to the digital realm: the influence of trading personalization for electronic rigor, the difference between understanding and

appropriation in digital vs. physical information environments, and the perceived threats as we move from a centralized to decentralized model for knowledge management.

The following chapter describes design implications for this analysis.

## 6 Privacy & Security Scenarios

In the previous chapter I discuss the data presented in Chapter 4 through three lenses to explore the embodiment of security and privacy into work practice, the communal nature of security in small centers, and the role that ambiguity plays in the management of sensitive client information.

In response to the analysis in Chapter 5 and to discuss solutions to the data presented in Chapter 4, this chapter is a collection and discussion of near-future scenarios demonstrating aspects of the possible design space.

Scenarios are powerful design tools. While the work preceding this chapter is deeply grounded in the practices, they are not responsive to design. Scenarios allow for a level of abstraction to then consider what is possible. They are stories about people, their interactions, and the tools that are used. They are user-centric, in that they describe the users interacting instead of the lifecycle of a tool. To quote Carroll, a founder of Scenario-Based Design, “Scenarios highlight goals suggested by the appearance and behavior of the system, what people try to do with the system, what procedures are adopted, not adopted, carried out successfully or erroneously, and what interpretations are people make of what happens to them” (Carroll 1999, p.2). Because of what scenarios can encapsulate, they serve as a valuable tool to present contributions for design.

I am presenting scenarios as spectrums. This builds off of the work of Chewar and McCrickard who argue that spectrums are useful for demonstrating a design space (Chewar et al. 2004; Chewar 2005; McCrickard et al. 2006). They argue that by examining the most extreme examples of contrasting factors in the designs space, the designer can illustrate the relevant issues. This, in turn, can lead to a better design.

The goal of these scenarios is to demonstrate and discuss the choices that future designs embody about how security and privacy will be managed in respect to the information system.

The spectrums are not presented to be exhaustive (like use cases), but as representative of example issues to consider within this information system design space (Carroll 2000).

### 6.1 *Assumptions Embedded Within the Scenarios*

There is a set of assumptions related to these scenarios that requires discussion before presenting the scenarios.

The first assumption is that technology will soon exist that will be able to track each person in the environment. This tracking software will know with certainty that person-n is in fact person-n. Whether this is through RFID scanning, a set of cameras in the environment that do facial recognition, or some other technical solution, the assumption is that there will be some technology that can do this.

For the purpose of these scenarios, I do not speculate on whether or not this technology can be circumvented. Indeed, RFID's can be hacked (Ilascu 2008), and facial scanning technology is not perfect (Pentland et al. 2000). The assumption, though, is that these will work.

The second assumption relates to the use of generic terms. Generic terms are used in the scenarios to abstract the particular location type. The assumption is that this abstraction will be helpful. While there are differences between childcare centers and physicians' offices, for the purpose of these scenarios the location type has been left ambiguous. Additionally, all teachers and health care workers are referred to as "staff." Directors of both centers are referred to as the director. Patients and parents are referred to as "client."

The third assumption is about circumvention. As discussed in previous chapters, when security mechanisms are not adopted at a local and individual level, they are circumvented, e.g., (Adams et al. 1999; Whitten et al. 1999). For the purpose of these scenarios, circumvention by the users is not accounted for. This is because any security mechanisms can be misused and misappropriated. The possibilities are only limited by imagination.

The last assumption is that these solutions represent something "better," where "better" is left nebulous. I am not arguing that any of these solutions in and of themselves represents the future direction for privacy and security in the management of sensitive client information. Instead, these scenarios are proposed as thought exercises to explore the different aspects of the design space.

## ***6.2 Scenarios Representing Spectrum Ends***

These scenarios use the same actors throughout. I will now present brief persona's to describe them:

**Alice:** Alice has worked at a center for many years and has high-level access to all client information, in contrast to others who work at her same center. She works with tools like phones, computers, ambient displays, and online record systems.

**Rosemary:** Rosemary works with Alice at the center, but has less access than Alice.

**Judy:** Judy works with Rosemary and Alice and has highly restricted access to information. She is also has questionable morality and generally is trying to access information she should not have access to.

**Reese:** Reese is a typical client who provides his personal information to the center. He has an account on ClientBook (described later).

### **6.2.1 Access v. Inaccess**

One of the most basic issues in security and privacy in these centers revolves around issues of access: who has access to what information at what time under what conditions? While this issue can be dressed up in many disguises, the basic premise is a spectrum

where on one side everyone can have access to all information and on the other side people do not have access to all information.

Based on the themes derived from the phenomenological analysis of the data, this spectrum represents responses to data from the themes Information Withheld or Hidden, Access Policy Work Arounds, Local Negotiation of Policy, Practice Performance Problems, Access Policy, and Sensitive Information Publically Available.

I present two scenarios where access and inaccess are juxtaposed:

**Access.** Alice hangs up the phone after talking with a client. While talking she was jotting down notes for things she is going to need to verify in the client's file before calling the client back. She then walks over to the filing cabinets containing all of the client's files, finds the client's file, and writes down the private information. However, she could not find everything. She goes over to the shared computer station to look at the client's electronic record. She quickly pulls up the record, verifies the information she already has, and finds the additional information that she needs. She then returns to the phone and returns the call of the client with the necessary information in hand.

**Inaccess.** Alice hangs up the phone after talking with a client. While talking she was jotting down notes for things she is going to need to verify in the client's file before calling the client back. She then walks to the room that holds the client's files and enters a personal door code. After she enters the room, she goes to the filing cabinets where she again has to enter a unique password to open the filing cabinets. Once she has found the file, she has to write her name on the outside of the file to log her access. She finds the information she needs and writes down the private information. However, she could not find everything so she goes over to the computer station to look at the client's electronic file. Before hand, she returns the file, and makes sure the filing cabinet is locked. She then enters her unique password into the computer. She pulls up the record, and can see the previous people who have accessed that file. She then verifies the information she already has, and tries to find the additional information that she needs. After examination, she realizes that can see that the information she needs is there, but that she cannot access it. She logs out of the computer, leaves the room while making sure that the room is locked, and passes a message to the director.

The two scenarios presented demonstrate relevant issues of access and inaccess. In the first scenario Alice demonstrates a case where there is open access and because of open access she is able to find and relay the information that she needs. Alternatively, in the other scenario, because of the restricted access to information she is not able to find the information that she needs.

These scenarios are juxtaposed to demonstrate a few key problems: the number of additional steps required to gain access to information in a system where access is limited; the need for additional actors who do have access when information is needed; and, the knowledge and reflection about the lack of access.

*The lack of access security barriers does not necessitate security breakdowns.* In the first scenario Alice is able to easily access the information and complete the task. In contrast to the first scenario, the second scenario shows Alice encountering numerous security barriers. In the second scenario Alice is also unable to complete the task individually. The tradeoff between the amount of time spent navigating security barrier should be considered when evaluating the other important work necessary in the centers.

*Visible access security mechanisms serve as reminders of privacy.* In the first scenario Alice's access to the information is fluid. Her only problem is finding the information in the correct location. In the alternative scenario Alice has a door password, a cabinet password, a paper log file, and an electronic password. All of these steps are interleaved to ensure the security of the information.

The presence of these steps serves a valuable function. It serves as a barrier to implicitly indicate that the information is private. Because there are protective mechanisms surrounding the information, the information is secure. In contrast, in the first scenario these indicators are lacking. This can imply that the client's information might not also be worthy of protection.

*Access security mechanisms can reinforce social work.* In the first scenario Alice is easily able to handle the task from start to end without the interaction with another person. However, in the second scenario Alice has to rely on another person to finish the task.

In these scenarios Alice's independence is both a problem and benefit. Similar to when a nurse is not able to find the location of a patient's file, the problem reinforces the community of security. In essence, the breakdown serves the function of enforcing the social relationships that are necessary for the work. By passing on the work to the director in the second scenario it reinforces that the director is the one in charge of the information, and that the director is the one with the authority. Additionally, by being able to validate who had previously accessed a file, Alice is conducting the valuable job of being social awareness of work.

### **6.2.2 Anonymity v. Visibility**

One of the central issues discussed throughout many of the breakdowns in Chapter 4 are issues related to the lack of visibility. For instance, individual passwords and log-ins were rarely used and workstations were shared and the visibility of access was minimal.

In paper systems there are natural affordances that decrease anonymity when managing client information. First of all, there is only one file. If a teacher cannot find a file it is because someone else has it. Second of all, people have unique handwriting that makes it

easier to distinguish who contributed to a client's record. Last, records have physical location that can distinguish who has previously managed the information (e.g., director's desk).

These affordances are missing in electronic systems and the work that people did do in an electronic system was fairly invisible. For example, one person in the office had little knowledge of what the person was actually looking at on their computer (contrary to paper records, where the visibility of what was being examined is more apparent to the surrounding people).

Based on the themes derived from the phenomenological analysis of the data, this spectrum represents responses to data from the themes Beliefs About Security, Human-Technology Mismatch, and Inadequate Representation in Available Information Systems.

In this section I present scenarios to discuss the spectrum of anonymity to visibility.

**Anonymity.** Alice is pulling client files from the shelves. From the corner of her eye she can see Rosemary working and typing. Alice does not know what Rosemary is currently working on. She thinks to ask, but she does not want to bother Rosemary as she is working. As Alice moves the files to her desk, she speculates that Rosemary might be handling work from a recent phone call or one of her normal tasks. To determine what Rosemary is doing, Alice enters the electronic system and attempts to look at the electronic file system for a recent phone call. She finds a file that was updated within the last minute. This allows Alice to infer what Rosemary was doing. Alice looks down at her client's files and starts to work through them.

**Visibility.** Alice is pulling client files when she looks over at Rosemary's computer. From the corner of her eye she noticed that its normal white color has started to shift to green. This indicates that Rosemary is currently in the electronic record system rather than using the computer for another task (e.g., checking email). As Alice moves the files to her desk she sees that Rosemary's computer has shifted from green to red, indicating that Rosemary is currently looking at client files that she does not regularly access. Alice quickly looks over at the ticker display on the wall. She can see that the last file accessed by Rosemary was from the client who recently called. Alice also notices that next to her icon on the display the number of times she has accessed the filing cabinets has incremented. She is currently in the lead, but this is normal. What is abnormal is the number of times that Judy has accessed the files this week, which spiked on Tuesday. Alice asks Rosemary, and Rosemary says that Judy was helping her with client files on Tuesday as a favor. As Alice sits down and starts parsing the client files, she peripherally notices that Rosemary's computer transitions to green and then white when Rosemary leaves the room.

These two scenarios demonstrate two different ends of the spectrum of anonymity and visibility. One scenario demonstrates how in going about her task Alice has little awareness of what her colleague is doing. Instead, she has to infer from prior activities and time-stamped files what Rosemary is doing. Contrary to that scenario, the next one provides Alice with numerous indicators of the work that Rosemary is doing and the degree of risk. These scenarios demonstrate four issues that are relevant to the spectrum of visibility and anonymity that are discussed below.

*Visibility affords awareness.* In either scenario there is a desire to know what the other person is doing. This does not mean that people are micromanaging other people's work. Instead, people in the offices kept a general awareness of tasks at hand and what needed to be accomplished; these were busy places! Orienting towards the other person was valuable. However, in order to orient, Alice needed to visibly see the work that Rosemary was doing. In the first scenario, the work that she does and the work that Rosemary does are anonymous. Contrary to that scenario, in the second one Alice has full awareness of her work, Rosemary's work, and of others in the office who have recently accessed the client files. The visibility of other's work affords awareness.

*Contextual knowledge is valuable.* In both scenarios Alice has to use her knowledge of the context to infer the work of Rosemary. It is not merely that the screen is green or that Alice can see that the client's file was modified within the last minute. These are contextual clues, but are limited. It is when Alice puts it all together that she is able to create contextual knowledge. For designers this means supporting enough clues to allow for meaningful inferences. By providing peripheral systems, the users can stay focused on her task while still being able to infer that Rosemary is handling a recent phone call. The importance of context and Alice's ability to evaluate that context is the power behind both scenarios.

*Both paper and electronic systems afford different kinds of visibility and anonymity.* One of the proposed benefits of electronic systems is the purported ease with which security of client information can be enacted. However, as shown in the first scenario, the electronic system does not afford visibility of the work of Rosemary. This decreases the ease with which Alice can validate her work. Similarly, paper-based systems do not afford easy ways to track who has touched what. This decreases the ease with which anyone in the office is able to track the paper files. The paper-based system affords decreased ability to track access without modification, and the electronic-based system affords decreased awareness. When used in combination, the designer needs to consider how to combat these weaknesses present in both systems in order to support how much visibility and anonymity is desirable.

*Awareness affords security.* Implicit in this discussion is the correlation between awareness and security. Without knowledge of what another person is doing, there is little ability to monitor and then enforce local policies surrounding the management of sensitive client information. Anonymity, on the other hand, affords the work of one functioning as the work of many, as discussed in Chapter 5 on Communities of Security.

This means that to design for the problems presented in Chapter 4, the designer must be sensitive to not overly distinguish between the work of individuals and provide sensitive methods of awareness. For example, gently changing the color of someone's computer to provide awareness of interactions is a lightweight and peripheral method of increasing awareness. Alternative choices would be to have the name of the patient's file displayed on the back of the computer monitor, or for a small part of another person's screen re-estate show the interactions of another in the office. The designer needs to weigh the trade off between allowing for work to still be anonymous, thus representing community-driven work, while still leveraging awareness for security.

### 6.2.3 Permanence v. Decay

Permanence was prevalent in the centers in this study. For example, files were kept for an indeterminate amount of time and access to those files was generally only ended when the person stopped working at the center. Passwords, additionally, when used, were never changed, and paper records were kept for every relevant piece of information "just in case."

Similarly, in reference to access, Sinclair et al. found that once granted access it was rarely revoked (Sinclair et al. 2007).

While permanence is prevalent in the centers, so was decay, but in a very rudimentary sense. Files that were past a certain age were generally moved into storage. This had the affordance of making them harder to access. Apart from this example, though, most information and access was permanent.

Based on the themes derived from the phenomenological analysis of the data, this spectrum represents responses to data from the themes Access Policy Work-arounds, and Information Withheld/Hidden, and Sensitive Information Publically Available.

In this section I present two scenarios to demonstrate the role of permanence and how access decay could be used in reference to the management of client information.

**Permanence.** An old client is returning to the center to re-start business. Alice quickly types in the client's name into the electronic database, but finds that she does not have access. She asks Rosemary what she should do, and Rosemary pulls up the file as well. Rosemary sees that the client's was last at the center 5 years ago. She quickly adds the client to the list of active patients, which everyone can see. Alice looks through the client's files, prepares the information that the client will need to provide, and exits the system. At three and six months, when the Alice needs to access this client's file again, she quickly pulls it up and makes the change.

**Decay.** An old client is returning to the center to re-start business. Alice quickly types in the client's name into the electronic database, but finds that she does not have access. Rosemary pulls up file only to see that the display is fuzzy; the information is hard to read. The system asks

Rosemary if she would like to re-activate the file. Rosemary says yes, but the older private information should be kept inactive. For example, the information documenting difficulties with this client should not be included in the client file. Additionally, Rosemary assigns the file specifically to the roles of office staff. Until the client officially returns, there is not a need for others in the office to have access. Once Alice has access she quickly looks through the files, prepares the information that the client will need to provide, and exits the system. In three-month time when Alice needs to access this client's file again, she finds that she cannot access it. The amount of time in between previous accesses has been too long and she has to request access again. In six months time she again needs to access the file, but this time another office staff has previously accessed the file intermediately. Since decay is associated with role rather than individual, Alice still has access. Alice quickly makes the change.

In these two scenarios the spectrum of permanence and decay are played with.

Permanence is an important value for the centers in the study. They want to be reliable and enduring, and this value pervades other aspects of their business. For example, centers allowed staff members to have permanent access and files existing indefinitely.

What I've proposed in these scenarios are different ways that decay can be used when juxtaposed with permanence. The benefit of permanence is its stability. Decay, on the other hand, adds additional layers into the system. These issues are discussed in more detail below.

*Decay embodies client privacy.* Decay is one method of attempting to insert more client privacy into the center's work practice. Instilling impermanence into the file, thus making it harder for people to access, ensures privacy. Much like the crumbling paper records, it creates a sense of delicacy in the management of the file. For example, the tool of graying out the record when it is past a certain age is borrowed from smudged ink in old documents. Similarly, creating barriers around accessing files after they have been unused is borrowed from the current model of packaging and removing older files. Mechanisms like these can help support the privacy of the information while still respecting the necessity of information.

*Decay is reliant on time, not context.* One problem with the proposed use of decay is its reliance on time. With the push for context aware computing, a computer system should be able to determine the person, situation, context, and need for the information and make a decision based on that need. However, what I propose is that time limits are strict. They serve as a visible barrier for accessing information and relay an implicit message about the importance of the use of that information.

The centers already use time as a marker for when clients are old. The use of more time markers provides additional layers that the centers are already comfortable with using.

In contrast, permanence is indefinite. It does not set a barrier for when to access information, but instead reflects a stability of the information.

*Decay and does not have to be individual.* There are many possible uses of decay, but one that I would like to focus on is the difference between individual decay and group decay. What might be old to one person does not mean that it is old to another. This fact is important for the client. After all, the client does not need to know that it was Alice rather than Judy who last modified their file.

In the second scenario Alice attempts to access the file after three months and is unable because no one else with her role has accessed that information within the decay's time limit. However, when she tries to access the file after an equal amount of time again she is able to access the file because someone else has.

This distinction is important. The use of roles in this way reflects the communal nature of work and it uses the power of role-based access. Instead of a person being assigned a role, and information being assigned to that role with permanence, decay is used to manage access and permanence.

#### **6.2.4 Centralization v. Decentralization**

There were many examples in the data where information about clients was centralized and decentralized. Particularly within childcare centers, information about the children was distributed within the environment. The most extreme of these breakdowns was in incidents where teachers had to document cases of child abuse. However, there were also examples in physicians' offices where information about patients was distributed across types of records kept for different purposes (e.g., billing and health records).

Multiple locations of information is a security threat due to the fact that it means that there are more locations to keep secure. However, as discussed in the previous chapter, multiple versions of the same file or information snippet are not just redundant; they serve a purpose. One of those purposes was to keep information private (away from prying eyes), but another is to keep information shared.

Based on the themes derived from the phenomenological analysis of the data, this spectrum represents responses to data from the themes Synchronizing Information with Reality, Information System Problems, Human-Technology Mismatch, Policy Violation, Information Acquisition, and Local Negotiation of Content.

In this section I present scenarios to discuss the spectrum of centralization to decentralization.

**Centralization.** It is the annual time in the center to check if information in client files has been updated. Alice sits down at her workstation (of which there are two for the entire center) and creates a list of all of the client's records she is going to have to validate and send out notifications.

Recently, her office became entirely paperless. This means that the database of client records she is accessing is the only location of client information. As she starts to work through the records she tries to access the file for a particular client. In doing so the display tells her that another person is currently accessing the record. Alice makes a note by that client and moves on to others. Later, she accesses the files again and makes the appropriate updates.

**Decentralization.** It is the annual time in the center to check if information in client files has been updated. Alice sits down at her workstation (of which there are many) and creates a list of all of the client's records she is going to have to validate. As she makes a change to a particular record, a notification is sent to her. It asks her if she would like to push out a notification of the update or not. She selects "yes," which sends a notification to all of the information systems that may hold that information. The information system in the office is aware of other systems, but not what information they actually hold. In another room, Rosemary is asked if she would like the information for that client updated. Additionally, it asks if she would like to push out the notification to any systems that her workstation is knowledgeable of. Similarly, other workstations are asked the same question until all the systems are updated (or purposefully not updated). When Alice comes to a file that someone else is accessing, Alice is not aware of this fact because her copy is a unique instance of that information. While the information between the two machines may be identical, they are treated as separate.

In these two scenarios the spectrum of centralization and decentralization are explored in reference to the management of sensitive client information.

The first scenario depicts one database being accessed by a limited number of computers, and only one computer can access a unique file one at a time. The information is centralized and limited by the one instance model of information.

In the second scenario information is highly dispersed. There is no central database, but merely a network of computers that may have knowledge of each other. All instances of client information are unique.

I now discuss relevant points in reference to the spectrum of centralization versus decentralization.

*Centralization values community; decentralization values individuality.* In the first scenario, the record system functions as communal watering hole. When people need access to information they have to go to the record system that is stored in a particular limited location; access to files is limited. Much like taking turns getting water, people have to share the same file and resources. This sharing enforces the sense of community.

In contrast, in the other scenario everyone has individual versions of different pieces of information. There also is no central database, and there are as many “work stations” as necessary. This distributed model of information enforces a sense of individuality. It enforces that if people do not want to share information they do not have to, while still supporting the distribution of information.

*Centralization values security; decentralization values privacy.* The second scenario has some relevant problems in reference to security. There are problems such as conflicting information (e.g., two people pushing out notifications that are not the same) or information not being updated to all of the necessary systems (e.g., the instance of the missing child).

However, the second scenario values privacy. It allows for people to maintain information that is unique to their needs (thus not overwhelming them with too much information), while also respecting the need for privacy in certain situations.

The first scenario, in contrast, has relevant problems in reference to privacy. With all information stored in one location, there is not an easy way to store information that others should not be able to access. Merely knowledge of the existence of the information could be a privacy breach (e.g., storing information on suspected abuse).

However, centralization embodies security. There are fewer items to manage and the information system more easily allows for robust information to be kept.

### **6.2.5 Layered v. Flat**

One of the tools used by the centers that were studied was the use of layers to manage privacy and access to information about clients. Post-it notes were particularly important for indicating temporary information about a client that might not be stored permanently. There were also observed instances of using multiple files, not just for different functions, but because it was difficult to manage the privacy of the information if it was stored in one location (e.g., Med-P17 storing information about a patient who had problems paying her bills). Childcare centers were additionally observed to store extra sensitive information about children towards the back of the file, in essence layering information to ensure security by obscurity.

The problem arises because while paper affords layering, electronic systems do not. There is one file that represents all of the official information about the client. With issues like the increase in patient agency, as was discussed in Chapter 5, the need for maintaining the privacy of the center along with the privacy of the client will be important. This means that considering layering in the design space is critical for privacy and security.

Based on the themes derived from the phenomenological analysis of the data, this spectrum represents responses to data from the themes Practice and Performance Problems, Local Negotiation of Content, and Access Policy.

In this section I present scenarios to discuss the spectrum of Layers to Flat.

**Layered.** Alice receives a message from an external office. A client has terminated their business with Alice's center. The people in the external office need a copy of the client's file for their records, but also for the client. Alice opens up the electronic file (her center is paperless), and looks at the file. She clicks the button to view the client-friendly record. It shows the initially provided enrollment information, dates and records of any incidents, appointments, and any relevant pictures. In one of the notes about an incident, Alice sees information that should not be shared. The note says that the client was "difficult." Alice goes back to the record, highlights the information, and selects to make that information only available to people at that office. She reviews the file again, and then selects to send that file to the external office for the client. She then views the client-friendly record, and selects to show specific details about the care about the client. She reviews this information, and sends this file for the external office's use. Alice then marks the file as expired.

**Flat.** Alice receives a message from another external office. A client has terminated their business with Alice's center. The people in the external office need a copy of the client's file for their records, but also for the client. Alice opens up the electronic file (her center is paperless), and looks at the file. She clicks on the button to export the file, and reviews the file. She sees that there is some information in the file about the client being difficult. She realizes that this might be difficult to explain, but could be useful for the other center. She sends that file over to the external office and then calls the other center to explain the circumstances. She then re-enters that information, and exits the system.

Hierarchies existed in the centers that were observed, with particular reference to an us-versus-them mentality of the office staff and clients. Access to information for those who were considered external was limited. This was not out of malice, but because the centers had a need to protect their own privacy.

The first scenario demonstrates how layering information could be used by the center to provide information to the client and to an external center. It also demonstrates that layering of information that may be useful for the centers.

Alternatively, the second scenario demonstrates what a flat system might look like. In this scenario all information centralized, everyone internal can access anything in the system, and all information is shared.

I now discuss relevant issues related to the contrast between the two scenarios.

*Layering affords hierarchy.* The protection of being able to layer information ensures privacy. It means that only certain people should be able to access certain information.

For example, in some cases the director is the only one who should be able to access expired client's files. In being able to layer information, and being able to visualize what information would be viewable by those in other roles, the user can ensure privacy. Layering also affords security because the hierarchy allows for information to be centralized, as discussed in the previous spectrum section.

*Flat affords distribution.* The second scenario demonstrates the outcome of a flat system: egalitarian access to information. Even information that is private and could get the center in trouble is regarded as possibly relevant to the other center and thus is shared. Similarly, if the client does not already know that they were marked as a difficult client, perhaps reading the file would help them establish better social skills. Whatever the reason, the value of sharing is on providing information, not in limiting it.

Within centers, flat systems afford a communal sense of information and client management: because everyone has equal access, all are responsible for maintaining and securing it. Similar to eavesdropping, there is a sense that all information is useful. This means that there is no distinction between external and internal people.

### **6.2.6 Contextual Awareness v. Lack of Contextual Awareness**

One way to manage many of the problems presented in Chapter 4 is to use a lot of technology. What would be necessary though is the degree of awareness of that the technology has of the context of the users. Prior research has explored what context means, and how context can change. However, when it comes to security and privacy, detecting the context can have variable meaning. Therefore, these scenarios play with the spectrum of contextual awareness in an attempt to examine what that system would look like.

Based on the themes derived from the phenomenological analysis of the data, this spectrum represents responses to data from the themes Policy Violation, Access Policy Work Arounds, Sensitive Information Publically Available, Practice and Performance Problems, Local Negotiation of Policy, and Inadequate Representation in Available Information System.

In this section I present scenarios to discuss the spectrum of Contextual Awareness to Lack of Contextual Awareness.

**Contextual Awareness.** Alice is looking at a client's record on her electronic system. She realizes that she does not understand a problem presented in the client's file, and asks Rosemary if she can figure it out. Rather than Rosemary coming over to her desk, Alice selects a button to show the record on the wall display. While discussing the problem, Judy enters the room. The system, which can detect Judy's presence, immediately grays out the display. (Judy does not have access to that client's information that is displayed.) When Judy leaves, the display returns. While discussing the client, Rosemary remembers another client with a similar problem. She says aloud, "Display Sam Williams." The

outline of Sam William's record, that anyone internal to the center is allowed to see, appears. The system prompts the two for a password. Rosemary asks Alice what is the password since she does not have access. Alice says the password to the system. The system then displays Sam William's record and sends an email to Alice with a new password. When they are done discussing the problem Alice tells the display to resume normal visual settings.

**Lack of Contextual Awareness.** Alice is looking at a client's record on her electronic system. She realizes that she does not understand a problem presented in the client's file, and asks Rosemary if she can figure it out. Rather than Rosemary coming over to her desk, Alice selects a button to show the record on the wall display. While discussing the problem, Judy enters the room. Alice picks up a remote and blacks out the display. When Judy leaves, Alice turns the display back on. While discussing the client, Rosemary remembers another client with a similar problem. Rosemary goes to her computer and tries to pull up Sam William's file but she does not have access. The system shows the information that anyone in the office can access, but not the information she needs. Rosemary asks Alice what the password is, and Alice tells her. The system displays Sam William's record and when they are done discussing the problem, Alice walks back to her workstation.

These two scenarios extend beyond the choice of more or less technology; it pushes back against the assumption that more technology is better. These scenarios represent choices about how much technology could and should be aware of the context of the users.

These ends of the spectrum represent how much people want to handle security and privacy manually. In a sense, inserting more steps into the process (social and technical) to make security and privacy salient is in contrast to a computing system handling all of the choices for the user.

I now discuss relevant issues related to the spectrum of contextual awareness versus lack of contextual awareness.

*People-centric and rule-centric policies are not the same thing.* In the first scenario, the responsibility for managing and enforcing security and privacy is in the hands of the technology. The users do not have to think about whether or not Judy should see the information, and when passwords are shouted. The system can detect these needs. Similar thoughts involve preventing eavesdropping by playing loud white noise when there are people present who should not hear what is being discussed. The system could conceivably be conscious of the context and could develop methods for adapting to keep client information safe.

In the other scenario, the users have to make conscious choices in the moment, of who should see what information. This does not mean that all information is shared, but more

enforce the important local and negotiated decisions about access. Policies such as these are impermanent, individual, and social. More importantly, they are people-centric rather than rule-centric applications of privacy.

*Balancing the need-to-know with privacy.* In both the first and second scenarios Rosemary is aware that there is a similar problem in another client's file, but is unable to access it. How this problem was managed was variable by scenario. In the first scenario the system recognized that the password has been shared, thus supporting the need for on-the-fly policies without demanding the work stop. However, the extra cognitive work of remembering a new password can be a hindrance to Alice. In the second scenario Alice had to provide her password to Rosemary, but the system had no way to know that Rosemary is now seeing information that she should not be able to see. Instead, what is being relied on is Alice's understanding of the contextual needs to supply information for Rosemary.

*Contextual Awareness supports nefarious activities, but prohibits communal awareness.* Many of the security and privacy breakdowns that were discussed in Chapter 4 were not malicious. However, this does not mean that malicious use of information does not exist. Contextual awareness can help spot nefarious activities more effectively in certain ways. They can help spot unusual circumstances, they can spot breaks in routine more easily, they do not become tired, nor are they subject to charm (Flechais et al. 2005). They can spot someone hiding behind a door listening to a conversation; and, they can monitor interactions with client files. These are positive aspects of the use of contextual awareness.

On the other hand, many of them prohibit communal awareness. Perhaps when Judy overhears Alice and Rosemary's conversation she would be able to help them later. Enforcing security policies to protect client information inhibits the shared nature of the work.

### **6.2.7 Center-managed Privacy v. Client-managed Privacy**

Patient agency is increasing and adapting how we think about the management of client information. Additionally, legislation and external policies are shifting to adapt to the increasing changes in patient agency. For example, HIPAA states that patients have the right to view their medical records, and that they can correct any information in the record.

With patients, as one type of client, gaining agency the question becomes who is going to be responsible for managing the client's information and privacy. As demonstrated in the data, teachers are already starting to store information about children on their Facebook profiles. Additionally, medical students have been observed storing information about patients on their profiles (Cohen 2011). How is the expansion of privacy and information management going to be accounted for?

In these scenarios I present two sides of the spectrum of client's managing the privacy of their information, and center's managing the privacy of client information. One important

assumption in these scenarios is that clients would and could be granted access to client information, and that they would want to have access to it. To help visualize these scenarios I provide Figure 23. This figure is a user interface similar to Facebook, and for the purpose of this visualization it presents medical information for “Reese Client.”

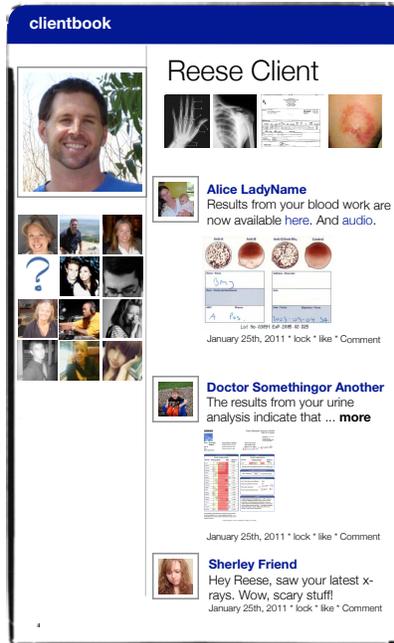


Figure 23. A hypothetical user interface similar to Facebook for managing client information.

Based on the themes derived from the phenomenological analysis of the data, this spectrum represents responses to data from the themes Policy Violation, Access Policy Work Arounds, Information Acquisition, Information System Problems, Information Withheld or Hidden, Access Policy, and Sensitive Information Publically Available.

In this section I present scenarios to discuss the spectrum of center-managed privacy to client-managed Privacy.

**Center-managed Privacy.** Alice logs into ClientBook, a website like Facebook, but for clients to manage their information. Reese, a client, has requested a copy of notes from his last meeting with the center. Alice pulls up Reese’s record. This record shows Reese’s picture with his demographic information along the top. Along the left-hand side she can see the other people at the center who have access, along with people from outside the center who have been granted temporary access to Reese’s file. She goes to the audio from Reese’s recent meeting and listens to the recording. She then tags Reese as being able to access this information with a time limit of 30 days. After providing access, she adds a note that only her, her boss, and Reese can see information about a question he had last time he was there. After she is finished she decides to review Reese’s

file to see who has recently accessed it. She can see that Judy and Rosemary have accessed his file to post billing information. Additionally, she can see that Reese has shared access with a friend. Alice selects this person's access and sets a decay of 30 days. With her task complete she exits his record.

**Client-managed Privacy.** Reese logs onto ClientBook, a website like Facebook, but for clients to manage their information. He types in his name and his password and is shown his picture with his demographic information along the top. Along the left-hand side he can see the businesses that have access to his sensitive personal information. He needs to look at the audio from a recent meeting with one of the centers. He clicks on that center and finds the recording of the meeting, which only he and people from that center can access. After listening to the recording, he shares the recording with his family members. He marks that they are able to access that record indefinitely. Reese can see that someone from the center recently added a note to the recording. He reads the note, but then marks it as private and restricts access. While he is on the ClientBook he decides to review who has looked at his file. He can see that various people have accessed his file while posting billing information. However, he notices that someone named Alice has been accessing his file frequently without any visible changes. He marks Alice as having restricted access until he is contacted personally.

In both of these scenarios the actors are restricting access to client information to specific actors and sharing information with others. The difference exists in the goals that are represented in the actions. Reese desires to share information with family members, but not all information. Reese also questions a center staff's access of his files and is allowed to restrict access. Contrary to the second scenario, Alice only shares part of Reese's information with him restricting the client's access to their information to what is requested and not the whole file.

I now discuss relevant issues related to the spectrum of client-managed privacy versus center-managed privacy.

*Access reflects ownership.* For these scenarios the responsibility of managing privacy reflects ownership of the information. In the second scenario Reese can restrict access and provide access to any information that is associated as his. In this scenario that went as far as restricting office staff to his information because his trust was breached. Similarly, in the first scenario Alice provides and restricts access to information that is stored in Reese's record. In both of these cases, Reese and Alice can restrict access because they essentially own the information. It is theirs to manage, and therefore the onus to protect and manage the information relies on the owner.

*Ownership is ambiguous.* Both of these scenarios directly contradict the current method of managing client information. This reflects a zone ambiguity over the ownership of the

information and the responsibility to manage the information. For example, many parents believed that they were the owners of the information, or shared ownership. In these scenarios, in contrast, only one party has the ability to make final decisions about who can access and modify information about the client. By one person making specific designations of who can see what information, who owns the information is no longer nebulous.

*Centers share responsibility among the staff members; a client is only one person.* One of the clearer differences between the two scenarios is the distribution of responsibility. When the responsibility of monitoring access is the clients, there is only one person. Contrary to that, when the center is responsible for monitoring access, there are many people who can monitor access. It is easier for one person to make mistakes versus a team of people. However, the client is personally invested in managing their information. Again, this is different for a team of people where a policy can be created but not necessarily followed.

*Sharing access to external people.* In both scenarios Reese has shared his sensitive information with external people such as his friends and family. One of the problems presented in Chapter 4 was that doctors and teachers shared information with external people without obtaining the consent of the patient. In the client-managed privacy model, this problem is no longer left ambiguous. In this instance the client either provides access or they do not. However, in the alternative scenario, the client can have limits placed on whom they want to share information with.

### **6.2.8 Technical v. Social Enforcement**

In the previous sub-sections all of the scenarios depict some kind of technical intervention to solve the problems presented in Chapter 4. However, not all solutions have to be technical. The centers are socio-technical spaces. This is demonstrated even in the scenarios with technical interventions: people interact, share sensitive information, and orient towards each others work.

The goal of this section is to present alternative solutions that are social in nature to manage the problems presented in Chapter 4. For this reason, the all of the other scenarios are representative of the technical side of the spectrum and the following scenario represents the social side of the spectrum.

Based on the themes derived from the phenomenological analysis of the data, this spectrum represents responses to data from the themes Social Relations Problems, Beliefs about Security, Human-Technology Mismatch, Access Policy, and Information Acquisition.

In this section I present scenarios to discuss the spectrum of technical to social enforcement.

**Social Enforcement.** Nancy is visiting a center for her monthly, unannounced inspection. She enters and asks for Alice. Alice is the newly

appointed local administrator for managing the security and privacy of her client's information. Nancy explains that this is the monthly inspection, but she was also notified that a client was unsatisfied with how their information was managed. Alice shows Nancy her weekly re-issuing of passwords, her auditing of 5% of the files, and the citations she issued to people that week for leaving their computer stations open. Nancy reviews these and also starts to check 5% of the client files. Afterwards she inspects the place, the location of the files, and writes a citation for information being left out of the client's file. She then asks for access to Sam William's file. Nancy reviews the access log and validates that there were numerous accesses to Sam's file without annotations or change to the file. There was also a download of the file without permission from the client. Nancy asks Alice about these problems, and Alice explains that she was unaware of the problem. Nancy issues a citation with a fine. Nancy then leaves, enters her notes into her system, and contacts Sam William about the outcome of his filed complaint.

In this scenario the management and enforcement of security is social. Instead of technology systems re-issuing passwords, or validating access, two people in the scenarios specifically enforce policies.

I now discuss two important points relevant to the spectrum of social and technical enforcement.

*Social application of rules affords negotiation.* One of the interesting observations between the childcare center licensor and the director was how the licensor did not issue citations for problems she saw. This is because social systems involve negotiation and leverage relationships. In the observation breakdown, the licensor trusted that the problems she saw would be quickly mitigated. Ostensibly, in issuing the citation, she would be doing more harm than good. (After all, as shown by her prior record available on the Virginia DSS website, she does not have problems issuing citations to other childcare centers.)

In this scenario citation writing and the application of external rules are still individually appropriated. If Nancy had determined a probable reason why Sam's file had been accessed, she would not have issued a citation. This is as positive application of social systems: their inherent flexibility and ability to respond to contextual needs.

*Technical systems and social systems have different methods of enforcing compliance.* The consequences for not following an electronic security system are that the users have to go through extra procedures. It can be bothersome, but the worst consequence is a tax on time. This is because electronic systems procedures are preformed every time: the user is always prompted for a password; and, a person will always be denied access.

Electronic systems have no way to recognize when their policies have not been followed. This means that they do not have any way to issue citations. Social systems, in contrast, can recognize when rules have been broken and can use laws to enforce compliance.

### **6.3 Discussion**

#### **6.3.1 Seamless and Seamful**

Passwords are a kind of seam. They are places in the socio-technical system where the transition from action to goal is inhibited by a seam. Many of the breakdowns that were discussed and observed were ones involving a lack or misuse of passwords. In this chapter numerous responses have been presented that demonstrate user's having to enter more passwords, as in Section 6.2.1, and ones where shouting passwords is supported, as in section 6.2.6. These passwords function as a barrier to the information but also as a reminder that what is about to be accessed is private.

The differences in the number of seams that have been introduced into the system serves as a background discussion between these scenarios. Should security be seamful or seamless? There are two sides of this argument.

The first is that if more seams were introduced into the management of sensitive client information, this cognitively affords reminding the center staff that the information they are managing is sensitive. Additionally, because barriers are used the information is more protected, thus more secure.

The other side of the argument states that if too many seams are introduced or if the seams are done in a way that impedes with the work, users find ways to circumvent them. Additionally, there were centers that had passwords but chose not to use them. It might be better to instead remove passwords all together, and instead support security through other mechanisms that are seamless. For instance, instead of a user logging into a computer, the computer detects the user and logs them in securely.

Another difference is in social versus technical seams in regards to security. Social systems appear seamless. People are not asking each other for a password, and sadly, the secret handshake has been relegated to spy fiction. When people were observed to ask for a password, they were provided with it, and there were only a handful of times where people were actually denied access to information.

However, there were seams in the social system, they were just so intrinsic to the system that they appeared natural. Whispering was used to hide information, additional files were created in the information system, folders were closed, etc.

Contrary to this, electronic systems appear seamful. Electronic systems have obvious error messages, they stop interaction, and they enforce policies. They are not natural seams, but can be bothersome for the task.



Figure 24. Sample of an electronic seam.

Designers of socio-technical secure systems need to consider how seams can be used to highlight the need for privacy, while not creating such obvious and encumbering seams that result in obfuscation by the user.

### 6.3.2 The Surveillance of Security

Many of the scenarios and assumptions embedded in this chapter are about surveillance. It is assumed that the people who work in these centers, as a type of user, will accept having their interactions studied, noted, and reported. Without providing a value judgment of the merits of surveillance (which other research has adequately discussed (Booker et al. 2010)), there are two problems that should be discussed.

A surveillance protocol should be created, training should be provided, and auditing should be used if a center's staff is going to be monitored. The protocol should discuss how data will be stored, who will have access to it, how the storage device will be protected, where data will be stored after it is processed, what data is collected, how it is processed, and the longevity of the information. Also included should be the amount of control that the users can have over what data is collected about them, meaning that they should be able to delete data at any time. (Many of these issues parallel issues about client's being able to review their own information.)

The second problem related to the conscious choice to use surveillance systems. Given that most of this dissertation has been about supporting privacy and security of the client, little effort has been spent considering the privacy of those who work in the centers. Do companies who manage sensitive information have a right to privacy? What about the individuals who work there? Do employee's have the right to privacy? If someone accesses my information, what rights and information do I get to learn about them? The power balance between what is known about providers and clients is unbalanced currently. This fact reflects the little that is known about how sensitive information is actually managed.

### 6.3.3 "Do Nothing" Scenario

Implicit in response to each of the scenarios presented in this chapter is the alternative "do nothing" scenario.

The current system works. People get their work done, children and patients are cared for, and the information management. Despite the evidence presented in Chapter 4 and in

the Appendix, the system is relatively secure. After all, there were no truly critical incidents, but just many anxiety-producing breakdowns (e.g., ordering a life-ending test for a patient; a missing child). Everything was resolved, even if it was resolved in a way that would be unsatisfactory if clients knew more about information management practices (thus disturbing the zone of ambiguity).

In creating a new design solution it is difficult to recognize all of the ways that the new solution may influence how people work. This fact is more crucial within security systems where the misuse of security protocols can result in privacy and security problems. For instance, the use of the computer CD tray as a cup holder is a problematic use of the technology, but one with few negative social ramifications. Alternatively, when physician's office staff start selling the medical records of the rich and famous to the tabloids, e.g. (AssociatedPress 2009), the ramifications are a little larger. Or, when physicians' offices move out of a location, they need to be able to pack all of their client's medical records, e.g. (Karas 2010).

The circumvention, misappropriation, misapplication of the proposed security and privacy design solutions can result in insecure systems. This is not to say that the perfect design solution could never be misused. My argument is the alternative to this statement.

All systems can be misused. The difficulty is designing a system that intrinsically will not be misused, circumvented, misappropriated, misapplied. This involves deeply understanding the values and current work practices of the people who are being designed for. Creating a new system that does not embody the problems discussed in Section 5.1 (care, individuality, local, and robustness of information) is one that is going to be circumvented. In deed, that is why passwords were rarely used, shouted, and shared; the use of passwords, a security mechanism, did not actually embody the social work that people need to do thus resulting in circumvention.

In designing any solution it is critical to consider not only how to prevent circumvention, but what will be done to increase adoption at local and individual levels. After all, it only takes one person to make an entire socio-technical system insecure. In considering how a possible solution could be circumvented, and comparing it to the current system, a list of pros and cons can be derived that can highlight whether the risk of circumvention is too high. For instance, open access without auditing may be acceptable for an office of two people, but for an office of 40 or 4,000 people, the design decision may overwhelm the need for security.

#### **6.4 Summary**

In this chapter I have presented eight spectrums that represent a response to the breakdowns presented in Chapter 4.

These scenarios demonstrate the tensions that exist in the design space and how they could be responded to. In particular, they attempt to elucidate the different concerns that are going to exist as technology is increasingly adopted into the socio-technical systems that were studied. How to manage access versus inaccess when balancing the need for

collaboration is a difficult problem. These scenarios can be used when considering how to approach hard problems like the ones in Chapter 4.

Additionally, I have presented three concerns and discussion points as a meta-analysis to these scenarios. First, I discuss seamless and seamful. The introduction of seams or the lack there of was different depending on the spectrum to be considered. This means that seams will be embodied based on the larger need represented in the scenario.

Second, I discuss the problem of surveillance. Given the underlying assumption of concern as an advocate for patient privacy, the designer must not forget that the people in this design space also have a right to privacy. Without respecting the privacy of the people who work in these centers their adoption of the system will be questionable.

Last is the question of the ‘do nothing’ scenario, in which the designer has the choice to not create any new solution. This scenario is not stating that there is not a consequence for doing nothing, but merely that it is a solution that is rarely considered. In reference to security and privacy, it is important to consider how practices can and will be affected with new solutions, and whether or not these practices are worse or better than what might occur without a new solution.

These three concerns should be considered when designing; however, they cannot stand alone without the spectrums to truly understand the design space.

## 7 Conclusion

In this dissertation I have provided six chapters that have presented a phenomenological analysis of security and privacy in childcare centers and physicians' offices as examples of places that manage sensitive client information. I have walked the hallways and corridors of centers, discussed how information is managed, and accounted for how security and privacy have been embodied.

The primary work of childcare centers and physicians' offices is to manage the care of their patients. One of the primary findings from this dissertation is how security and privacy are entwined in the care of clients. When the provision of care came in conflict with security and privacy, either at the local or individual level, the socio-technical system broke down. Security and privacy were most effective when they embodied care, robustness, and were locally and individually adopted. However, there were circumstances where electronic system's policies and rules, because of their recent use in the centers that were studied, had not been established.

In my introduction I presented Figure 1, which depicted overlapping spheres of social and technical mechanisms for managing security and privacy. Additionally, I argued that electronic systems are failing to account for how sensitive personal information is being managed socially, thus resulting in systems where the social nature of this work is neglected.

To respond to these discussed problems, in Chapter 4 I provided examples of problems with the electronic systems that demonstrate critical issues in relation to security and privacy. In essence, when the technical system did not account for how centers want to manage their work (which was efficiently, but socially) centers found ways to *make* the electronic system work for them, even if it resulted in security breakdowns.

Chapter 5 then demonstrated how social systems could be used in conjunction with electronic systems in different ways to facilitate both technical and social mechanisms to create secure practice. While there was no definitive answer to all breakdowns presented in this dissertation, the scenarios presented in Chapter 5 are places to start converging social and technical solutions.

Throughout this document the research questions presented in the introduction have been answered. I now present summary points for each sub-question:

- *What breakdowns happen when the explicit and implicit rules are not followed?*  
The appendix includes a list of all breakdowns in relation to security and privacy and a summary is provided in Chapter 4. To understand the essence of security and privacy, themes were derived that speak to the types of breakdowns that were discussed and observed. These span from usability problems that can be corrected with simpler interfaces, such as relying on knowledge workers memory to recall codes, to extremely social problems such as office staff engaging in disputes that affected the management of client information and care. However, a large set of

problems revolved around synchronization. For example, there were problems related to electronic and paper systems, but also across social and technical systems. With the information system distributed and messy, many breakdowns revolved around the theme that, due to conflicting objectives, numerous information sources were created that were hard to account for. Future work should extend past considering individual breakdowns as units to examine, but to instead consider the entire system. The themes presented in Chapter 4 are initial work in this direction.

- *How are breakdowns accounted for, negotiated, and managed in socio-technical systems where sensitive personal information exists?* An important finding is that no one died and no child was abducted during the collection of this data. All clients were cared for. However, there were some particularly anxiety-inducing observations of children being temporarily missing and a receptionist catching a patient's life being put in jeopardy due to an ordered procedure. These breakdowns highlight that even in extreme circumstances, solutions were found, negotiated, and managed using the social and technical tools at hand. However, most solutions to breakdowns resulted in a compromise in client information. For instance, instead of client information being disposed of after a client left the center, client information was kept indefinitely. There was no negotiation, and clients assumed that their information was being destroyed. This breakdown example highlights that when a breakdown occurred, the result was usually that client security and privacy were compromised. This occurs because the care of the client is the primary objective of the centers. When these two goals were in conflict, privacy and security were ignored.
- *What are the implicit and explicit rules surrounding how physicians' offices and childcare centers handle sensitive personal information?* Policies such as HIPAA and licensing regulations from the Department of Social Services represent the most external and explicit rules. There were also local explicit rules that were outlined in privacy policies and handbooks that patients and parents had to sign. There were additionally local implicit rules such as not entering the director's office, and rules that were embodied in the roles that people played. Last, there were individual implicit rules that people followed regarding how they believed client information should be managed. When these rules were in conflict, breakdowns occurred. Knowing what the rules are, and how they were followed provided an important layer in examining security and privacy. However, security and privacy was found to be more than rules (or when rules came into conflict). The broader function of security and privacy encapsulates identity, accountability, and care.

Overall, client information is managed with two purposes in mind: supporting the business and supporting care for the client. In reference to security and privacy, these constructs were embodied into the social nature of security. Work in the centers that were studied is accounted for socially so that the work of one person functions as the work of many. Additionally, because of the intricate work of the centers, there was a need for

improvised choreography in regards to security and privacy. The community had to adapt together, because one person acting as an individual would result in security breakdowns.

Additionally discussed in this dissertation is the topic of zones of ambiguity which reflect the tenuous relationship between sharing knowledge along with the need to keep some knowledge unknown. Zones of ambiguity in regards to security and privacy facilitate the social relationships and messiness of work, while still allowing the centers to manage information in a secure way.

The purpose of this work has been to examine the body of data collected comprising of interviews and observations childcare centers and medical physicians' offices in the New River Valley of Southwest Virginia.

The results from this study have been presented to provide insight into producing electronic and social security mechanisms that support collaborative work practice.

With this summary in mind I now present three closing point: the argument between paper and electronic records, future work, and reflections on the research project.

### ***7.1 Paper versus Electronic Client Files***

Part of the discussion in the background of this dissertation has been the debate between paper and electronic client files. While the purpose of this dissertation is not to make that distinction, or to say that one is better than the other, the debate does serve as the background to this dissertation.

There are people who provide anecdotal evidence, along with research evidence saying that electronic records are the future for providing robust, secure, timely, and accurate information about clients (Hippisley-Cox et al. 2003; 2010d; Rowe 2010; Janes 2011). Similarly, there has been equal evidence about the troubles with electronic records such as workload, fears of surveillance, and cost (Hackl et al. 2009; Merrill 2010; Ofri 2010). As the emergence and use of electronic records become more or less pervasive, security and privacy mechanisms will need to adapt to them. The important aspect for designers to recognize is that changes will have to be accounted for in the socio-technical system, and to recognize that merely applying more rules will not account for the larger issues demonstrated in this dissertation.

In Conway et al.'s paper he compares 10 years of evolution in regards to patient safety. In the paper one of the more important discussion points was the changing perspectives of the community (Conway et al. 2006). Within ten years the belief that errors are rare resolved to the belief that errors are everywhere. Similarly, the onus of errors has changed in respect to placing blame and firing people, adding more checks to engaging with patients, finding the root causes, and simplifying the system.

These changes in ideology reflect the importance of the role that technology has on daily practice. With new legislature, changing attitudes towards technology, and rising health

costs, the perceptions of what role technology can and should play in physicians' offices and childcare centers are going to change.

What is necessary is for the argument about paper versus electronic to dissipate. The question is not whether paper is better or electronic systems are better, but the discussion should be about what each system affords. Currently, office staff members have acclimated and learned methods to account for their work through paper. And, apart from the acclimation, paper has some natural affordances that electronic systems do not. Examples include being folded, grabbed and hidden quickly, and laid. Electronic systems, while arguable easier to share, and arguably easier to enforce security mechanisms, have a long way to catch up to support the social work that paper naturally affords.

So instead of arguing paper or electronic, designers should look at the current socio-technical and support it with the tool that meets the needs of the users.

## ***7.2 Future Work***

There are at least two important pieces of information that might prove instrumental to the design of usable and secure information managements systems that are still mostly unexplored: the ways in which information is physically managed already and the social environments in which technical solutions might be deployed.

With these points in mind, future work should continue to look at current socio-technical systems to understand how social mechanisms account for failures in the technical systems, and how technical systems are accounting for social security mechanisms. In the broader realm of person and group information management system, this means thinking beyond the high amount of work that has come out of looking at electronic medical record systems, but to also consider systems such as childcare centers, employee records, and criminal and public records. These domains each have unique own accounts of security practice that are valuable for designing new technical systems.

The body of data that was collected spans thousands of pages. The data presented in this dissertation is only one part of that larger body of data that covers the culture of the centers, the power distribution between office staff, and the workflows of information management. Future work could additionally use different analysis methods to study the body of data relevant to security and privacy in other ways such as through the use of grounded theory and content analysis to provide different insights.

In discussion of this research with others there have been additional questions that were interesting but outside the scope of this work. The most interesting of this is to interview parents of children who have unresolved medical problems about security and privacy.

Additionally, there are questions about how to handle client information in emergency situations, and about the social life of sensitive information versus the electronic life.

The largest area of future work is building technology probes to explore the different scenarios presented in Chapter 6. For example, I envision a wizard of oz type study where an office setting is replicated and then directors from childcare centers and physicians' offices are asked to participate in the study. They could be asked to act out the different scenarios and then reflect on how the different technology mechanisms influenced their work and also the security and privacy.

A last piece of future work would be to actually study the artifacts that exist in these offices. As to date, I have been unable to find any study that examines one client file and then details who has touched it, when, why it was accessed, and secondary implications for that access. This study and others have shown that looking at access logs does not necessarily visualize who actually looked at the client's information (since people share workstations, and passwords). Following one artifact as it moves through the office would shift the focus away from the people and their work, as was the purpose of *this* dissertation, onto the artifact.

### **7.3 Researcher Reflections**

The work represented in this dissertation is a bit discursive. This is because of the interdisciplinary nature of the work being situated between HCI, security, and medical informatics. On one side the multidisciplinary nature of the work means that there are many places to publish, but on the other side, this means that there is more research to discover and analyze in reference to this work than is possible within the scope of the dissertation. From HCI there is a deep body of research on the importance of context, and understanding the value placed on certain technologies; from security there is a deep body of research on threats and how to respond to them, along with many models on how networks respond; and, from medical informatics there stems this deep need to understand the role of technology in care along with a phenomenological history of body and tool. Together, these areas make a very large research project, yet one that has been deeply engaging.

Second, the number of people who have helped collect the data in this study is unusual. Including myself, there have been eight research students helping collect and analyze the data. The benefit is that there was copious discussion around the research topic, and in describing the research project to each person the project evolved into something stronger. The downside is that even with training there were inconsistencies in the data. Particular researchers had a tendency to focus on more workflow style data, and other researchers were more focused on describing the interactions rather than the surroundings. The differences in data influenced the method that could be used to analyze the data. To understand culture or to create a theory, for instance, consistent descriptions would have been necessary due to the requirements of rigor.

However, thousands of pages of data were collected. This again was a gain and a bane. There is so much data that to not focus on security and privacy breakdowns would have paralyzed my progress. However, it also meant that there were numerous examples that could be used to discuss any issue. The constraints of security and privacy in essence liberated the analysis of the data to focus on a microcosm of issues present in a much

larger body of work. The need for focus early on was a necessity for progress, but perhaps a weakness in that there might be more salient issues that would have emerged with further analysis.

There were considerable problems recruiting participants. While the researchers that I worked with and I did not have to metaphorically “strong arm” any participants, we had to be very diligent in setting up meetings with participants. One childcare was contacted seven times until a final meeting time was set up for the first interview.

However, just because participants agreed to be interviewed did not mean that they would then agree to participate in observations. There was considerable hesitation for repeated observation with many centers refusing to return my calls or saying that they would think about it and call me later (yet never doing so). This meant that there are many practices that were not included in my data, and I suspect ones that are much less “secure” than even what was observed.

The people who did participate were honest, but also told me like it was, with one director reflecting that she cries because she has so much work. I found this honesty amazing, but at the same time had to reflect on what I would have been able to see in the observations of people who were not so forthcoming. Would they take their work so seriously?

The lack of open participant was true of all locations apart from Child-P06, where my partner and I decided to enroll our child. This allowed me to informally continue my observations as a participant in the socio-technical system. During my official observations I was told that I could come at any time and stay for as long as I liked, I was never asked to leave, and I was gossiped with.

Being able to be active as a participant, and valuing my individual experiences was a benefit for the use of Phenomenology as a method. I believe it added to the research rather than detracted from my ability to be objective about the study. However, this is a kind of messy data collection. I had to be careful to distinguish my subjective experiences when analyzing the data.

A third concern in my work was the combination of childcare centers and physician’s offices. To study one fully, as I was told, is difficult enough. To then compare and contrast the experiences within and between is too much for a single dissertation. I was told that I could not do both meaningfully. I listened to this concern, because to respect the settings I was studying is important. However, my goal was not to study physicians’ offices or childcare centers. I wanted to study how sensitive information is managed, and this not done at one location. To truly speak to this larger area, I had to engage, at least initially, in both types of locations.

Future work should engage in an ethno-methodological analysis of only childcare centers and only physicians’ offices, or even just one childcare center or one physician’s office to

extend this research topic. This is not to discount the work presented in this dissertation, but to present a weakness and for future work.

One issue that is embedded with this work is the distinction between “is” and “ought.” People ought to use passwords, and they ought to not leave patient information unaccounted for. People ought to lock their filing cabinets, and not shout patient information. There are many things that people *ought* not to do. However, that is not the goal of this work. Instead, as technologists, it is our responsibility to represent the *is* in the socio-technical system.

In many discussions with people who I like to call “more technical in nature” I get responses to my work saying, “if only we made more rules, people would just comply.” What they mean is that if only we issued more sanctions and reprimanded people more, that they would suddenly start behaving the way they are supposed to.

Similarly, my work has been disregarded as too local and situated. Or, to put it more bluntly, that this is just a case of “country bumpkins” behaving badly. Not only is this a disservice to the fact that most of childcare centers and physicians’ offices in America might be classified as rural and rural serving, and thus as country bumpkins, this does not take into account the very real and busy working situations that these people find themselves in daily. There is too much work for people to be worry about entering in dozens of passwords. Additionally, people do not naturally have the cognitive capacity to manage the very important work they are doing and to then recall Machiavellian password requirements. Instead, as designers, we need to understand the value of care in reference to security, and understand how to design for the larger socio-technical system.

The last reflection is on the nature of this research topic. Given the interdisciplinary nature of the research there have been few scientific publications on this specific topic. I myself have had trouble publishing this work with feedback similar to, “good work, but not appropriate for this venue.” However, there have been numerous blogs, websites, reports, and news articles that have demonstrated the need and value for the work. This has meant shifting the landscape for studying a phenomenon. To study this issue the relevant landscape of literature is no longer going to be only peer-reviewed scientific articles, but also the many other resources that can lend insight into the issue to be studied. Part of the researcher’s job is going to be synthesizing emerging trends in topics like the one of this dissertation.

## 8 References

1. (2005) "Percentage of Children Ages 0-6, Not Yet in Kindergarten by Type of Care Arrangement and Child and Family Characteristics, 1995, 2001, and 2005." *ChildStats.gov*.
2. (2006). "Virginia Board of Medicine." Retrieved February 5th, 2011, 2011, from <http://www.vahealthprovider.com/>.
3. (2007a). "Learner-Centered Psychological Principles " Retrieved September 24th, 2007, 2007, from <http://www.apa.org/ed/lcp2/lcp14.html>.
4. (2007b). Virginia County GCT-T9-R. Housing Units (geographies ranked by estimate) U.S. Census Bureau.
5. (2008). Virginia Rural Health Plan.
6. (2009). "Working Parents: Parents in the Labor Force." Retrieved March 17th, 2010, 2010, from <http://www.catalyst.org/publication/252/working-parents>.
7. (2010a). "Child Day Care Overview." Retrieved June 2009, 2010, from <http://www.dss.virginia.gov/family/cc/index.html>.
8. (2010b). The Health Information Security and Privacy Collaboration Toolkit, Agency for Healthcare Research and Quality.
9. (2010c). "National Association for the Education of Young Children." Retrieved February 15th, 2010, 2010, from <http://www.naeyc.org/>.
10. (2010d) "Remote/Mobile Health Monitoring Holds Potential." *PriceWaterhouseCoopers*.
11. (2010e). "Understanding Health Information Privacy." Retrieved February 8th, 2010, 2010, from <http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>.
12. Aarts, Jos (2001). On Articulation and Localization - Some Sociotechnical Issues of Design, Implementation and Evaluation of Knowledge Based Systems. *Proceedings of the 8th Conference on AI in Medicine in Europe: Artificial Intelligence Medicine*, Springer-Verlag: 16-19.
13. Ackerman, Mark, Trevor Darrell and Daniel Weitzner (2001). "Privacy in Context." *Human-Computer Interaction* 16(2): 167-176.
14. Ackerman, Mark S. and Lorrie Cranor (1999). Privacy Critics: UI Components to Safeguard Users' Privacy. *CHI '99 Extended Abstracts on Human Factors in Computing Systems*, Pittsburgh, Pennsylvania, ACM.
15. Adams, Anne and Ann Blandford (2005a). "Bridging the Gap Between Organizational and User Perspectives of Security in the Clinical Domain." *International Journal of Human-Computer Studies* 63(1-2): 175-202.
16. Adams, Anne, Ann Blandford, Dawn Budd and Neil Bailey (2005b). "Organizational communication and awareness: a novel solution for health informatics." *Health Informatics Journal* 11(3): 163-178.
17. Adams, Anne and Martina Angela Sasse (1999). Users Are Not the Enemy. *Communications of the ACM*. 42: 40-46.
18. Aggarwal, Khushbu (2010). "The Relationship Between Pharmaceutical Companies and Physician's." *Berkeley Scientific Journal* 13(2).

19. Agre, Philip. E. (1994). "Surveillance and Capture." *Information Society* 10(2): 101-127.
20. Aita, Virginia, Diane M. Dodendorf, Jason Lebsack, Alfred F. Tallia and Benjamin Crabtree (2001). "Patient Care Staffing Patterns and Roles in Community-Based Family Practices." *The Journal of Family Practice* 50(10).
21. Arcand, Manon, Jacques Nantel, Mathieu Arles-Dufour and Anne Vincent (2007). "The Impact of Reading a Web Site's Privacy Statement on Perceived Control Over Privacy and Perceived Trust." *Online Information Review* 31(5): 661-681.
22. AssociatedPress (2009) "Ex-hospital worker convicted in patient record leaks dies." *Los Angeles Times*.
23. Baker, Aubrey, Laurian Vega, Tom Dehart and Steve Harrison (2011a). Healthcare & Security: Understanding & Evaluating the Risks. *Human-Computer Interaction International*. Orlando, Florida, United States, Springer.
24. Baker, Aubrey, Laurian Vega, Tom Dehart and Steve Harrison (2011b). Medical Record Privacy: Is it a Facade? *ACM CHI Conference on Human Factors in Computing Systems (CHI'11)*. Vancouver, British Columbia, Canada, ACM.
25. Barab, Sasha A., Michael A. Evans and Eun-Ok Baek (2004). Activity Theory as a lens for characterizing the participatory unit. *Handbook of research for educational communications and technology*. D. H. Jonasses. Mahway, NJ, Lawrence Erlbaum: 199-214.
26. Bardram, Jakob (2005). Activity-Based Support for Mobility and Collaboration in Ubiquitous Computing. *Ubiquitous Mobile Information and Collaboration Systems*: 166-180.
27. Bardram, Jakob (2009a). A Novel Approach for Creating Activity-Aware Applications in a Hospital Environment. *Human-Computer Interaction – INTERACT 2009*: 731-744.
28. Bardram, Jakob E. (1997). Plans as Situated Action: An Activity Theory Approach to Workflow Systems. *ECSCW '97*, Copenhagen, Denmark, Kluwer Academic Publishers.
29. Bardram, Jakob E. (2009b). "Activity-based computing for medical work in hospitals." *ACM Trans. Comput.-Hum. Interact.* 16(2): 1-36.
30. Bardram, Jakob E. and Claus Bossen (2005). "Mobility Work: The Spatial Dimension of Collaboration at a Hospital." *Computer Supported Cooperative Work (CSCW)* 14(2): 131-160.
31. Bardram, Jakob E., Jonathan Bunde-Pedersen, Afsaneh Doryab and Steffen Sørensen (2009). CLINICAL SURFACES - Activity-Based Computing for Distributed Multi-Display Environments in Hospitals. *International Conference on Human-Computer Interaction*, Uppsala, Sweden, Springer-Verlag.
32. Baron, Richard J. (1985). "An Introduction to Medical Phenomenology: I Can't Hear You While I'm Listening." *Annals of Internal Medicine* 103: 606-611.
33. Baskerville, Richard, Jan Stage and Janice I. DeGross (2000). *Organizational and Social Perspectives on Information Technology*, Springer.
34. Beck, Hall P., Sharman Levinson and Gary Irons (2009). "Finding Little Albert: A Journey to John B. Watson's Infant Laboratory." *American Psychologist* 64(7): 605-614.

35. Beech, Sarah, Erik Geelhoed, Rachel Murphy, Julie Parker, Abigail Sellen and Kate Shaw (2003). The Lifestyles of Working Parents: Implications and Opportunities for New Technologies. *HP Labs Technical Reports*, HP.
36. Bellotti, Victoria and Abigail Sellen (1993). Design for Privacy in Ubiquitous Computing Environments. *Conference on Computer-Supported Cooperative Work*, Kluwer Academic Publishers.
37. Benotsch, Eric G., Seth Kalichman and Lance S. Weinhardt (2004). "HIV-AIDS Patients' Evaluation of Health Information on the Internet: The Digital Divide and Vulnerability to Fraudulent Claims." *Journal of Consulting and Clinical Psychology* 72(6): 1004-1011.
38. Berner, Eta S., Don E. Detmer and Donald Simborg (2005). "Will the Wave Finally Break? A Brief View of the Adoption of Electronic Medical Records in the United States." *J Am Med Inform Assoc* 12(1): 3-7.
39. Bødker, Susanne (1996). Applying Activity Theory to Video Analysis: How to Make Sense of Video Data in Human-
40. Computer Interaction *Context and Consciousness*. B. A. Nardi. Cambridge, Massachusetts, MIT Press: 147-174.
41. Booker, Queen Esther and Fred L. Kitchens (2010). "Changes in employee intention to comply with organizational security policies and procedures factoring risk perception: A comparison of 2006 and 2010." *Issues in Information Systems* XI(1): 649 - 658.
42. Bossen, Claus (2002). The parameters of common information spaces:: the heterogeneity of cooperative work at a hospital ward. *Computer supported cooperative work*, New Orleans, Louisiana, USA, ACM.
43. Branham, Stacy, Monika Akbar and Laurian Vega (2009). Process and Situated Practice: The Unofficial Rules of Childcare Information Management. Blacksburg, Virginia, Virginia Tech.
44. Bredekamp, Sue and Teresa Rosegrant (1992). *Reaching Potentials : Appropriate Curriculum and Assessment for Young Children* Washington DC, National Association for the Education of Young Children.
45. Brustoloni, José Carlos and Ricardo Villamarín-Salomón (2007). Improving security decisions with polymorphic and audited dialogs. *Proceedings of the 3rd symposium on Usable privacy and security*. Pittsburgh, Pennsylvania, ACM: 76-85.
46. Bylund, Markus, Kristina Höök and Alina Pommeranz (2008). Pieces of Identity. *Nordic Conference on Human-Computer Interaction*, Lund, Sweden, ACM.
47. Cabitza, Federico, Marcello Sarini, Carla Simone and Michele Telaro (2006). Torres, a Conceptual Framework for Articulation Work across Boundaries. *Proceeding of the 2006 conference on Cooperative Systems Design: Seamless Integration of Artifacts and Conversations -- Enhanced Concepts of Infrastructure for Communication*, IOS Press: 102-117.
48. Carayon, Pascale (2006). "Human factors of complex sociotechnical systems." *Applied ergonomics* 37(4): 525-535.
49. Carroll, John M. (1991). The Kittle House Manifesto. *Designing Interaction: Psychology at the human-computer interface*. J. M. Carroll. New York, Cambridge University Press: 1-16.

50. Carroll, John M. (1999). Five Reasons for Scenario-Based Design.
51. Carroll, John M. (2000). *Making Use: Scenario-based Design of Human-Computer Interactions*. Cambridge, Massachusetts Institute of Technology.
52. Chewar, C. M. (2005). User-Centered Critical Parameters for Design Specification, Evaluation, and Reuse: Modeling Goals and Effects of Notification Systems. *Computer Science*. Blacksburg, Virginia Tech. **Ph.D.:** 294.
53. Chewar, C. M., Edwin Bachetti, D. Scott McCrickard and John E. Booker (2004). Automating a Design Reuse Facility with Critical Parameters: Lessons Learned in Developing the LINK-UP System. *Computer-Aided Design of User Interfaces IV*, Funchal, Madeira Island, Portugal, Kluwer Academic Publishers.
54. Chowdhury, M. M. R., J. Noll and J. M. Gomez (2007). Enabling Access Control and Privacy through Ontology. *Innovations in Information Technology, 2007. IIT '07. 4th International Conference on*.
55. Cialdini, Robert B. (2001). *Influence: Science and Practice*. Needham Heights, MA Allyn & Bacon.
56. Clark, Margaret S. (1984). "Record keeping in two types of relationships." *Journal of Personality and Social Psychology* 47(3): 549-557.
57. Clark, Margaret S., Judson R. Mills and David M. Corcoran (1989). "Keeping Track of Needs and Inputs of Friends and Strangers." *Pers Soc Psychol Bull* 15(4): 533-542.
58. Clark, Margaret S. and Barbara Waddell (1985). "Perceptions of Exploitation in Communal and Exchange Relationships." *Journal of Social and Personal Relationships* 2(4): 403-418.
59. Coburn, Andrew F., A. Clinton MacKinney, Timothy D. McBride, Keith J. Mueller, Rebecca T. Slifkin and Mary K. Wakefield (2007). "Choosing Rural Definitions: Implications for Health Policy." *Rural Policy Research Institute Health Panel*.
60. Cohen, Randy (2011) "When Med Students Post Patient Pictures." *The New York Times*.
61. Convertino, Gregorio, Dennis C. Neale, Laurian Hobby, John M. Carroll and Mary Beth Rosson (2004). A laboratory method for studying activity awareness. *Proceedings of the third Nordic conference on Human-computer interaction*. Tampere, Finland, ACM Press.
62. Conway, James B., David G. Nathan, Edward J. Benz, Lawrence N Shulman, Stephen E. Sallan, Patricia Reid Ponte, Sylvia B. Bartel, Maureen Connor, Dorthy Puhy and Saul Weingart (2006). Key Learning from the Dana-Farber Cancer Institute's 10-Year Patient Safety Journey. *American Society of Clinical Oncology*. Atlanta, GA.
63. Cranor, Lorrie Faith and Simson L. Garfinkel (2005). Security and Usability, Safari Books Online.
64. Creswell, John W. (2007). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Thousand Oaks, California, Sage Publications, Inc.
65. Creswell, John W. (2007). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Thousand Oaks, California, Sage Publications, Inc.
66. Cutler, David M. (2008) "The American Healthcare System." *Medical Solutions*.

67. Desjean-Perrotta, Blanche (1998). "Through Children's Eyes: Using The Shadow Study Technique for Program Evaluation." Early Childhood Education Journal 25(4): 259-263.
68. Dourish, Paul (2004). *Where the Action Is: The Foundations of Embodied Interaction*. Cambridge, Massachusetts, MIT Press.
69. Dourish, Paul and Ken Anderson (2006). "Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena." Human-Computer Interaction 21(3): 319-342.
70. Dourish, Paul, E. Grinter, Jessica Delgado de la Flor and Melissa Joseph (2004). "Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem." Personal Ubiquitous Computing 8(6): 391-401.
71. Egelman, Serge, Janice Tsai, Lorrie Faith Cranor and Alessandro Acquisti (2009). Timing is Everything?: The Effects of Timing and Placement of Online Privacy Indicators. *Proceedings of the 27th International Conference on Human Factors in Computing Systems*, Boston, MA, USA, ACM.
72. Ehn, Pelle (1988). *Work-Oriented Design of Computer Artifacts*, Lawrence Erlbaum Associates.
73. Engeström, Yrjö (1987). *Learning by Expanding: An Activity - Theoretical Approach to Developmental Research*. Helsinki, Orienta-konsultit.
74. Engeström, Yrjö, Reijo Miettinen and Raija-Leena Punamäki (1999). *Perspectives on Activity Theory*, Cambridge University Press.
75. Ferraiolo, David F. and D. Richard Kuhn (1992). Role-Based Access Controls. *15th National Computer Security Conference*, Baltimore.
76. Fischer, Gerhard (1994). "Turning breakdowns into opportunities for creativity." Knowledge-Based Systems 7(4): 221-232.
77. Flanagan, John C. (1954). "The critical incident technique." Psychological Bulletin 51(4): 327-358.
78. Flechais, Ivan, Jens Riegelsberger and M. Angela Sasse (2005). Divide and Conquer: The Role of Trust and Assurance in the Design of Secure Socio-Technical Systems. *Workshop on New Security Paradigms*, Lake Arrowhead, California, ACM.
79. Fogel, J. and E. Nehmad (2009). "Internet social network communities: risk taking, trust, and privacy concerns." Computers in Human Behavior 25(1): 153-60.
80. Friedewald, Michael, Elena Vildjiounaite, Yves Punie and David Wright (2007). "Privacy, identity and security in ambient intelligence: A scenario analysis." Telematics and Informatics 24(1): 15-29.
81. Friedman, Batya, Peter H. Kahn, Jr. and Alan Borning (2002). Value Sensitive Design: Theory and Methods. University of Washington, University of Washington, Computer Science and Engineering Department.
82. Friedman, Batya, Peter H. Kahn, Jr. and Daniel C. Howe (2000). Trust Online. *Communications of the ACM*. 43: 34-40.
83. Fruhling, Ann L. and Sang M. Lee (2006). "The influence of user interface usability on rural consumers' trust of e-health services." International Journal of Electronic Healthcare 2(4): 305-21.
84. Gammon, Katharine (2010) "Keeping Medical Data Private." *Technology Review*.

85. Garfinkel, Simson L. and Robert C. Miller (2005). Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express. *Proceedings of the 2005 Symposium on Usable Privacy and Security*. Pittsburgh, Pennsylvania, ACM.
86. Gee, James Paul (2005). Social Languages, Conversations and Intertextuality. *An Introduction to Discourse Analysis: theory and method*. J. P. Gee. New York, Routledge: 36-37.
87. Gellersen, Hans W., Albrecht Schmidt and Michael Beigl (2002). "Multi-Sensor Context-Awareness in Mobile Devices and Smart Artifacts." Mobile Networks and Applications 7(5): 341-351.
88. Glesne, Corrine (1992). Chapter 4, Making Words Fly: Developing Understanding from Interviewing *Becoming qualitative researchers: An Introduction*. White Plains, New York, Longman.
89. Good, Nathaniel S. and Aaron Krekelberg (2003). Usability and Privacy: A Study of Kazaa P2P File-Sharing. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Ft. Lauderdale, Florida, USA, ACM.
90. Greyson, B and I Stevenson (1980). "The phenomenology of near-death experiences." American Journal of Psychiatry 137: 1193-1196.
91. Guindon, R. and B. Curtis (1988). Control of cognitive processes during software design: what tools are needed? *Proceedings of the SIGCHI conference on Human factors in computing systems*. Washington, D.C., United States, ACM.
92. Hackl, W. O., A. Hoerbst and E. Ammenwerth (2009). "“Why the Hell Do We Need Electronic Health Records?”" Methods of Information in Medicine 50(1): 53-61.
93. Hancock, Jeff, Jeremy Birnholtz, Natalya Bazarova, Jamie Guillory, Josh Perlin and Barrett Amos (2009). Butler lies: awareness, deception and design. *Proceedings of the 27th international conference on Human factors in computing systems*, Boston, MA, USA, ACM.
94. Harper, R. H. R., M. G. Lamming and W. M. Newman (1992). "Locating systems at work: implications for the development of active badge applications." Interacting with Computers 4(3): 343-363.
95. Harrison, Steve and Paul Dourish (1996). Re-place-ing space: the roles of place and space in collaborative systems. *Computer supported cooperative work*. Boston, Massachusetts, United States, ACM.
96. Harrison, Steve and Deborah Tatar (2008). "Places: People, Events, Loci --- the Relation of Semantic Frames in the Construction of Place." Comput. Supported Coop. Work 17(2-3): 135-135.
97. Hart, P. and C. Saunders (1997). "Power and trust: Critical factors in the adoption and use of electronic data interchange." Organization Science 8(1): 23-42.
98. Hassanein, Khaled S. and Milena M Head (2004). Building Trust Through Socially Rich Web Interfaces. *the Second Annual Conference on Privacy, Security, and Trust (PST'2004)*, Fredericton, Canada.
99. Head, Milena M and Khaled S. Hassanein (2002). "Trust in e-Commerce: Evaluating the Impact of Third-Party Seals." Quarterly Journal of Electronic Commerce 3(3): 307-325.

100. Heckle, Rosa R. and Wayne G. Lutters (2007). Privacy implications for single sign-on authentication in a hospital environment. *Proceedings of the 3rd symposium on Usable privacy and security*. Pittsburgh, Pennsylvania, ACM: 173-174.
101. Heidegger, Martin (2008). *Being and Time*, Harper Perennial Modern Classics.
102. Hillgren, Per-Anders and Per Linde (2006). Collaborative articulation in healthcare settings: towards increased visibility, negotiation and mutual understanding. *Proceedings of the 4th Nordic conference on Human-computer interaction: changing roles*. Oslo, Norway, ACM: 301-310.
103. Hippisley-Cox, Julia, Mike Pringle, Ruth Cater, Alison Wynn, Vicky Hammersley, Carol Coupland, Rhydian Hapgood, Peter Horsfield, Sheila Teasdale and Christine Johnson (2003). "The electronic patient record in primary care, regression or progression? A cross sectional study." *BMJ* 326(7404): 1439-1443.
104. Hitchings, Jean (1995). "Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology." *Computers & Security* 14(5): 377-383.
105. Hong, Jason I., Jennifer D. Ng, Scott Lederer and James A. Landay (2004). Privacy risk models for designing privacy-sensitive ubiquitous computing systems. *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques*. Cambridge, MA, USA, ACM: 91-100.
106. Howard, Michael (2005). A Look Inside the Security Development Lifecycle at Microsoft. *MSDN Magazine*, Microsoft. **November 2005**.
107. Huang, Jingwei and Mark S. Fox (2006). "An ontology of trust: formal semantics and transitivity." *Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet* 156: 259 - 270
108. Humphries, William D., Dennis C. Neale, D. Scott McCrickard and John M. Carroll (2004). Laboratory Simulation Methods for Studying Complex Collaborative Tasks. *Proceedings of the Human Factors and Ergonomics Society 48th Annual Meeting (HFES '04)*. New Orleans, LA: 2451-2455.
109. Huntington, P., D. Nicholas, B. Gunter, C. Russell, R. Withey and P. Polydoratou (2004). "Consumer trust in health information on the web." *Aslib Proceedings* 56(6): 373-382.
110. Ilascu, Denisa (2008) "Judge Lifts Gag Order on MIT Subway Hack Case." *Softpedia: Hacking News*.
111. Janes, Jared (2011) "Medical records technology helps with drug recall." *The Monitor*.
112. Jha, A. K., T. G. Ferris, K. Donelan, C. DesRoches, A. Shields, S. Rosenbaum and D. Blumenthal (2006). "How common are electronic health records in the United States? A summary of the evidence." *Health Affairs* 25(6): w496-w496.
113. Kaelber, David C., Ashish K. Jha, Douglas Johnston, Blackford Middleton and David W. Bates (2008). "A Research Agenda for Personal Health Records (PHRs)." *J Am Med Inform Assoc*: M2547-M2547.

114. Kaptelinin, Victor (1995). Activity Theory: Implications for Human-Computer Interaction. *Context and Consciousness: Activity Theory and Human-Computer Interaction*. B. A. Nardi. Cambridge, Massachusetts, The MIT Press: 103-116.
115. Karas, David (2010) "Aetna's 'left-behind' files increase - 7,250 people affected to be offered credit monitoring as peace of mind provision." *NJ.com*.
116. Karoff, Helle and Stine Liv Johansen (2009). Materiality, practice, body. *Proceedings of the 8th International Conference on Interaction Design and Children*. Como, Italy, ACM: 238-241.
117. Kientz, Julie A. and Gregory D. Abowd (2009a). KidCam: Toward an Effective Technology for the Capture of Children's Moments of Interest. *International Conference on Pervasive Computing*, Nara, Japan, Springer-Verlag.
118. Kientz, Julie A., Rosa I. Arriaga and Gregory D. Abowd (2009b). Baby steps: evaluation of a system to support record-keeping for parents of young children. *Proceedings of the 27th international conference on Human factors in computing systems*, Boston, MA, USA, ACM.
119. Kientz, Julie A., Rosa I. Arriaga, Marshini Chetty, Gillian R. Hayes, Jahmeilah Richardson, Shwetak N. Patel and Gregory D. Abowd (2007). Grow and know: understanding record-keeping needs for tracking the development of young children. *Conference on Human Factors in Computing Systems (CHI'07)*, San Jose, California, USA, ACM.
120. Kleiner, B. M. (2004). "Macroergonomics as a large work-system transformation technology." *Hum. Factor. Ergon. Manuf.* 14(2): 99-115.
121. Kobayashi, Marina , Susan R. Fussell, Yan Xiao and F. Jacob Seagull (2005). Work coordination, workflow, and workarounds in a medical context. *Conference on Human Factors in Computing Systems (CHI'07)*, Portland, OR, USA, ACM Press, New York, New York.
122. Kuutti, Kari (1995). Activity theory as a potential framework for human-computer interaction research. *Context and Consciousness: Activity Theory and Human-Computer Interaction*. B. A. Nardi. Cambridge, MA, Massachusetts Institute of Technology: 17-44.
123. Larsen, Simon B. and Jakob E. Bardram (2008). Competence articulation: alignment of competences and responsibilities in synchronous telemedical collaboration. *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*. Florence, Italy, ACM: 553-562.
124. Light, Ann (2008). "Transports of delight? What the experience of receiving (mobile) phone calls can tell us about design." *Personal Ubiquitous Comput.* 12(5): 391-400.
125. Marcus, George E. (1998). *Ethnography through Thick & Thin*. Princeton, New Jersey, Princeton University Press.
126. Mazurek, Michelle L., J. P. Arsenault, Joanna Bresee, Nitin Gupta, Iulia Ion, Christina Johns, Daniel Lee, Yuan Liang, Jenny Olsen, Brandon Salmon, Richard Shay, Kami Vaniea, Lujo Bauer, Lorrie Faith Cranor, Gregory R. Ganger and Michael K. Reiter (2010). Access Control for Home Data Sharing: Attitudes, Needs and Practices. *Proceedings of the 28th international conference on Human factors in computing systems*. Atlanta, Georgia, USA, ACM: 645-654.

127. McCrickard, D. Scott and Christa. M. Chewar (2006). Designing Attention-Centric Notification Systems: Five HCI Challenges. *Cognitive Systems: Human Cognitive Models in Systems Design*. C. Forsythe, M. L. Bernard and T. E. Goldsmith, Lawrence Earlbaum.
128. McKnight, Harrison D. and Vivek Choudhury (2006). "Distrust and trust in B2C e-commerce: do they differ?" Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet 156: 482-491.
129. Merrill, Molly (2010) "Medicaid data breach 'like an onion'." *HealthcareITNews*.
130. Merrill, Molly (2011) "Kroll names top 10 data security issues for 2011." *HealthcareITNews*.
131. Meyer, Harris (2010) "Scribes are doctors' tech support." *Los Angeles Times*.
132. Miller, William L, Reuben R. McDaniel, Benjamine Crabtree and Kurt Strange (2001). "Practice Jazz: Understanding Variation in Family Practices Using Complexity Science." The Journal of Family Practice 50(10).
133. Mullender, Sape (1993). Protection. *Distributed Systems*, Addison Wesley Publishing Company.
134. Mwanza, Daisy (2001). Where Theory meets Practice: A Case for an Activity Theory based Methodology to guide Computer System Design. *INTERACT'2001: Eighth IFIP TC 13 International Conference on Human-Computer Interaction*, Tokyo, Japan, IOS Press (Oxford, UK).
135. Nardi, B. A. (2007). Placeless Organizations: Collaborating for Transformation. *Mind, Culture, and Activity*. **14**: 5-22.
136. Nardi, Bonnie A. (1995). *Context and Consciousness: Activity Theory and Human-Computer Interaction*. Cambridge, Massachusetts, The MIT Press.
137. Nardi, Bonnie A. (1996). Studying Context: A Comparison of Activity Theory, Situated Action Models, and Distributed Cognition. *Context and Consciousness: Activity Theory and Human-Computer Interaction*. B. A. Nardi. Cambridge, Massachusetts, MIT Press: 69-102.
138. Nardi, Bonnie A. (1998). Concepts of Cognition and Consciousness: Four Voices. *ACM SIGDOC Asterisk Journal of Computer Documentation*.
139. Niles, Nancy J. (2010). *Basics of the U.S. Health Care System*, Jones and Barlett Publishers, Inc.
140. Nissenbaum, Helen (2004). "Privacy as Contextual Integrity." Washington Law Review 79(1).
141. Norman, Donald A. (1981). "Categorization of Action Slips." Psychological Review 88(1): 1-15.
142. O'Connell, Brid and David Frohlich (1995). Timespace in the workplace: dealing with interruptions. *Conference companion on Human factors in computing systems*. Denver, Colorado, United States, ACM: 262-263.
143. Ofri, Danielle (2010). The Doctor vs. the Computer. *Well*. T. Parker-Pope, The New York Times. **2010**.
144. Oldenburger, Kristen, Xinran Lehto, Richard Feinberg, Mark Lehto and Gavriel Salvendy (2008). "Critical purchasing incidents in e-business." Behav. Inf. Technol. 27(1): 63-77.

145. Palen, Leysia and Paul Dourish (2003). Unpacking "privacy" for a networked world. *Conference on Human Factors in Computing Systems (CHI'03)*, Ft. Lauderdale, Florida, USA, ACM.
146. Park, Sunyoung, Heeyong Jeong and John Zimmerman (2009). ENSURE: Support for Parents in Managing their Children's Health. *Proceedings of the Conference on Design and Emotion*, Hong Kong, The Design and Emotion Society.
147. Pentland, A. and T. Choudhury (2000). "Face recognition for smart environments." *Computer* 33(2): 50-55.
148. Petroski, Henry (1985). *To Engineer is Human: The Role of Failure in Successful Design*. New York, St. Martin's Press.
149. Pettersson, John Sören, Simone Fischer-Hübner, Ninni Danielsson, Jenny Nilsson, Mike Bergmann, Sebastian Clauss, Thomas Kriegelstein and Henry Krasemann (2005). Making PRIME usable. *Proceedings of the 2005 symposium on Usable privacy and security*. Pittsburgh, Pennsylvania, ACM: 53-64.
150. Pinner, Robert W. (1998). "Public health surveillance and information technology." *Emerging Infectious Diseases* 4(3): 462 - 464.
151. Polanyi, Michael (1966). *The Tacit Dimension*, Doubleday.
152. Premkumar, G. and Margaret Roberts (1999). "Adoption of new information technologies in rural small businesses." *Omega* 27(4): 467-484.
153. Raeithel, A. (1996). From Coordinatedness to Coordination Via Cooperation and Co-construction. *Workshop on Work and Learning in Transition*, San Diego.
154. Reason, James (1990). *Human Error*. Cambridge, Cambridge University Press.
155. Reddy, Madhu C., Paul Dourish and Wanda Pratt (2006). "Temporality in Medical Work: Time also Matters." *Comput. Supported Coop. Work* 15(1): 29-53.
156. Reddy, Madhu and Paul Dourish (2002). A Finger on the Pulse: Temporal Rhythms and Information Seeking in Medical Work. *Conference on Computer Supported Cooperative Work (CSCW'02)*, New Orleans, Louisiana, USA, ACM.
157. Ren, Yuqing, Sara Kiesler, Susan R. Fussell and Peter Scupelli (2007). Trajectories in Multiple Group Coordination: A Field Study of Hospital Operating Suites. *Proceedings of the 40th Hawaii International Conference on Systems Science*
158. Rittel, Horst (1972). On the Planning Crisis: Systems Analysis of the First and Second Generations, reprint #107 from *Bedrifts Okonomen*, no. 8, Berkeley, Institute of Urban and Regional Development, University of California.
159. Rosenberger, Robert (2007). "The phenomenology of slowly-loading webpages." *Ubiquity* 2007(April): 1-1.
160. Rowe, Jeff (2010) "Security isn't always a technical problem." *HITechWatch*.
161. Saltzer, Jerome H. and Michael D. Schroeder (1973). The Protection of Information in Computer Systems. *Fourth ACM Symposium on Operating System Principles*.
162. Schmidt, Kjeld and Carla Simone (1996). "Coordination Mechanisms: Towards a Conceptual Foundation of CSCW Systems Design." *Computer Supported Cooperative Work (CSCW)* 5: 155-200.

163. Sheeran, Louise (2000). Users' models of the internet. *CHI '00 extended abstracts on Human factors in computing systems*. The Hague, The Netherlands, ACM.
164. Simon, Herbert A. (1996). *The Science of the Artificial*, MIT Press.
165. Sinclair, Sara, Sean W. Smith, Stephanie Trudeau and M. Eric Johnson (2007). Information Risk in the Professional Services – Field Study Results from Financial Institutions and a Roadmap for Research, Dartmouth College.
166. Spafford, Eugene. H., Richard. A. DeMillo, Andrew Bernat, Steve Crocker, David Farber, Virgil Gligor, Sy Goodman, Anita Jones, Susan Landau, Peter Neumann, David Peterson, Douglas Tygar and William Wulf (2003). Four Grand Challenges in Trustworthy Computing, Computer Research Association.
167. Spradley, James P. (1979). *The Ethnographic Interview*, Harcourt, Brace, Janovich.
168. Strauss, Anselm (1988). "The Articulation of Project Work: An Organizational Process." *The Sociological Quarterly* 29(2): 163-178.
169. Strauss, Anselm, Shizuko Fagerhaugh, Barbara Suczek and Carolyn Wiener (1985). *Social Organization of Medical Work*, University of Chicago Press.
170. Suchman, Lucy (1987). *Plans and Situated Action*. New York, NY, Cambridge University Press.
171. Sudbeck, L. E. (2006). "Placing court records online: Balancing the public and private interests." *Justice System Journal* 27(3): 268-285.
172. Suddaby, R. (2006). "From the editors: What grounded theory is not." *Academy of Management Journal* 49(4): 633-633.
173. Thuraisingham, Bhavani (2005). "Security standards for the semantic web." *Computer Standards & Interfaces* 27(3): 257-268.
174. Toombs, S. Kay (1987). "The Meaning of Illness: A Phenomenological Approach to the Patient-Physician Relationship." *Journal of Medicine and Philosophy* 12(3): 219-240.
175. Trist, Eric L, Fred E Emery, Hugh Murray and Beulah Trist (1997). *The Social Engagement of Social Science: A Tavistock Anthology : The Socio-Ecological Perspective*, University of Pennsylvania Press
176. Turner, Phil (2005). "Affordance as context." *Interact. Comput.* 17(6): 787-800.
177. Vaidyanathan, Ganesh and Steven Mautone (2009). "Security in dynamic web content management systems applications." *Commun. ACM* 52(12): 121-125.
178. van Manen, Max (1990). *Researching lived experience: Human science for action sensitive pedagogy*. New York, State University of New York Press.
179. Vega, Laurian (2010). Security in Practice: Examining the Collaborative Management of Personal Sensitive Information in Childcares and Medical Centers. *Computer Science*. Blacksburg, Virginia Tech. **Ph.D.:** 104.
180. Vega, Laurian and Laura Agnich (2009a). Medical Practices Study Report. Blacksburg, Virginia, Virginia Tech.
181. Vega, Laurian, Stacy Branham, Steve Harrison and Dennis Kafura (2010). Securing Sensitive Information in Work Practice. *Human Computer Interaction Consortium (HCIC'10)*, Winter Park, Colorado, USA.
182. Vega, Laurian and Tom Dehart (2009b). Childcare Study Report. Blacksburg, Virginia, Virginia Tech.

183. Vuckovic, Nancy H., Mary Lavelle and Paul Gorman (2004). "Easedropping as Normative Behavior in a Cardiac Intensive Care Unit." JHQ Online Sept/Oct: W5-1 to W5-6.
184. Warren, Samuel D. and Louis D. Brandeis (1890). "Right to Privacy." Harvard Law Review 4(5): 193-193.
185. Whalen, Jack, Marilyn Whalen and Kathryn Henderson (2002). "Improvisational choreography in teleservice work\*." The British Journal of Sociology 53(2): 239-258.
186. Whitten, Alma and J. D. Tygar (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. *Proceedings of the 8th USENIX Security Symposium*.
187. Winograd, Terry and Fernando Flores (1986). *Understanding Computers and Cognition: A New Foundation for Design*. Norwood, New Jersey, Ablex Publishing Corporation.
188. Wyche, Susan P., Camila M. Magnus and Rebecca E. Grinter (2009). Broadening UbiComp's Vision: An Exploratory Study of Charismatic Pentecostals and Technology Use in Brazil. *UbiComp*, Orlando, Florida, USA, ACM.
189. Zhou, Li, Christine S. Soran, Chelsea A. Jenter, Lynn A. Volk, E. John Orav, David W. Bates and Steven R. Simon (2009). "The Relationship between Electronic Health Record Use and Quality of Care over Time." J Am Med Inform Assoc 16(4): 457-464.
190. Zhou, Xiaomu, Mark S. Ackerman and Kai Zheng (2010). Computerization and information assembling process: nursing work and CPOE adoption. *Proceedings of the 1st ACM International Health Informatics Symposium*. Arlington, Virginia, USA, ACM: 36-45.

## 9 Appendix A, Observed Breakdowns

All of the breakdowns involving client information management and security have been included in this document. The breakdowns are listed in the order they were discovered in re-reading the data. The data was roughly re-read in the following order: interview with physician's office directors, observations of physician's offices, interview with childcare center directors, observations of childcare centers, and interview with parents.

Locations and people have attempted to be made anonymous. Locations are given names such as ["Med"/"Child"]-P[Participant Number] where the location is either "med", meaning a physician's office, or "child", meaning a childcare center. People were given identifiers such as "PA1", or "Dr-PB2" which serves to distinguish between doctors and staff and also to indicate when people are at the same location, which is indicated by the second letter (e.g., PC1 and PC2 work at the same location).

For each breakdown type the format is the same. The titles of the breakdowns are only to serve as descriptors. Underneath each breakdown is a list of times where this type of breakdown was observed or with a list of people who discussed the breakdown during their interviews. Below this list is a brief description of the breakdown along with a short analysis of the causes of the breakdown through the lens of Activity Theory. Beneath the description is a list of possible design implications to respond to these breakdowns. Last, snippets from observation notes and transcripts are included to provide reference for the breakdown description.

Study 1 and Study 2 data have been separated.

### ***9.1 Getting Information that is Purposefully Not in the File (Study 2)***

Observed:

- Med-P17 2010-08-19 09:21AM
- Med-P17 2010-08-19 11:24AM

Not all information about a client is stored in their records (health/financial). This information is stored in the collective social knowledge base or in some other form in the center that is not an official client record. There were times when people were observed tapping that collective knowledge for more information about the client that they may not have direct access to.

For instance, there are times when PA1 from Med-P17 was being observed and she would be processing payments that had come in either through mail, from the office, or from the satellite offices. This breakdown type is about when she would notice that particular patients have a large bill and she would seek additional information about the patient from her colleagues in the office. If patients don't have around a zero balance, there was observed to be a note in the eMD file explaining what is happening with the patient's payment for services. PA1 would pull up this note, read through it quickly, and then close it. If the note was not sufficient she would then call PA5, who was down with

patient information, to get more information. Even though all PA1 had to do was process the payment that had come in, she could have been attending to other tasks that are relevant for the business (e.g., turning the patient over to a collection agency).

Analyzing the situation from an AT standpoint, there are issues of division of labor and tool support. The objective of PA1's task is to process payments. A breakdown occurs because the eMD tool is not storing relevant information that is known about a patient yet is not being stored in their electronic record for PA1 to be able to access. Instead of her being able to pull up that information herself in the file, she has to use social methods to access information about how the patient is paying their account. While there is a division of labor across PA5 and PA1 for managing this kind of payment information, it is disrupting PA1's primary task, of processing payments, to retrieve this information through a secondary channel. Reasons that this information isn't being stored in the electronic file may be because the tool does not support storage of this information, or that the privacy of the patient is being respected. To explain further, everyone in the office can access the eMD system. The information about how the patient is paying the bill may be information that only PA5 and PA1 can access. To keep that information private, the only way to get the additional information is for PA1 to call PA5.

#### Design Implications:

- Create a section of a patient file that stores what might be considered irrelevant information
- Allow for layering of patient information so that only certain people can access additional information.

#### Med-P17 Observation notes:

*2010-08-19 9:21 PA1 picks up the phone and what she is doing is starting to make sense. She calls someone, I don't know who, and is talking about a patient who looks like she is paying down a bill. She talks in hushed tones, and says that this patient used to owe over \$2000 but it is now down to around \$335. She hangs up the phone after agreeing with who is on the phone that this patient is doing very well. I believe that this is probably PA5 who is down in accounting... PA1 gets up and runs the envelope with the invoice to the patient through a large 3-4 foot machine that prints postage on envelopes. So what has happened here is that PA1 is putting in payments. She puts in a payment for this person who had a bill for over two thousand dollars, but is down to a reasonable amount. She calls someone, I think Lori, to talk about how this patient is paying her bill. She then prints an invoice, puts it in a letter, writes down the patient's address, and feeds it through the postage machine.*

*2010-08-19 11:24 PA1 is on the phone with someone about a patient who has a charge for about \$1700 total for shots. I ask about it. L tells me that PA5 was on the phone... It turns out that the patient came in and refused to go to the state to get them to pay for the immunizations and was determined to have them done at the doctor's office. The problem is that the state is free, and if they are done here, and they aren't the normal shots, then they have to charge them. They don't*

*charge them the cost of the visit, just the shot. But this patient was determined not to go to the state even though she already had a considerable amount that was due. So the patient got \$400 worth of shots, which made the total come to about \$1700. PA1 called PA5 to ask why the patient wouldn't go to the state when the bill was too big. There was a note in the file that said the patient was adamant. I don't think there was ever a conclusion about what was going to happen to this patient, but more that PA1 just wanted to know why they are letting the mother continue to rack up a large bill.*

## **9.2 Incorrect or Unresolved Information in the Patient File (Study 2)**

Observed

- Med-P15 2010-08-18 1:26PM
- Med-P15 2010-08-18 2:33 – 2:39PM
- Med-P17 2010-08-19 9:35AM
- Med-P15 2010-07-01 11:35AM

There are places in patient files where upon review it, someone in the office realizes that the patient's information is not complete. For instance, when the patient is paying for their bill, the office staff person realizes that she does not have her current insurance information, or when mailing the patient realizes that she does not have their address. Finding and rectifying this incorrect or unresolved information can only be accomplished by human surveillance, and is a clear place where technology could support, but cannot automate.

In the first example, PC1 from Med-P15 is entering in information from paper files into the electronic system, and realizes that PC3 has entered the wrong information in for that patient's address. Instead of putting in 'xxxx's like PC1 says is appropriate, PC3 had put in something "joke-like" as an alternative. While PC1 was able to detect the wrong information, and track down that it was in fact incorrect through social means, the wrong information was associated with a patient for a period of time. This breakdown is caused by an insufficient rule as to what to do when the patient's address is unknown, and the computer system (tool) not supporting unknown information.

In the second example, PC4 from Med-P15 receives a call from a physician's office that shares a patient with them asking for a patient's new phone number. When PC4 is finally able to track down the patient's file, look up the patient's phone number, and call back the office, it is only then that she finds out that they both have the incorrect phone number. However, little more is done to the patient's file than PC4 noting that the patient's phone number is incorrect.

In a third example from Med-P15, the ladies in the front office discuss a patient who recently had left. The patient was one that was referred to them, and the file said that the patient would be female. Instead this was a case where a man had a female name. The ladies in the front office explain that this happens when the other office does not require the patients to fill out gender on their papers. Then someone along the way

has to make a guess as to the gender of the patient, and because of the name they guess incorrectly.

In a forth example, similar to the observation in ‘Getting Information that is Purposefully Not in the File,’ when a patient came to the window to check out, PA1 from Med-P17, a front office knowledge worker, would go through a regular procedure. She would ask the parent for the name of the child. Strangely, she did not ask for the name of the child. I have to assume that this is because names can be so easily misspelled and children can have similar names, whereas birthdays are fairly unique. After PA1 is done typing in the birthday, a series of children for that birthday come up. PA1 then makes a suggestion as to the name of that child to the parent. All except one time was PA1 accurate in her guess, and the one time PA1 was incorrect either the parent said the wrong birthday or PA1 misheard. PA1 would then pull up the eMD file and tell the parent how much they have to pay.

In the instance covered below in the observation notes for Med-P01, PA1 had noticed that this patient had a note in their record. After reading the note in the record, she realizes that she does not have the correct insurance information for the child. For this patient, the case gets a little complicated, because the child, who is the patient, is covered by both her mom and her dad’s insurance, and they are divorced. The information in the note roughly says that the insurance information is an old card. Based on PA1’s knowledge of insurance companies, she knows that this insurance company has switched to a new name, but cannot remember. By stringing together her knowledge and by calling PA5, she is able to reconstruct that she needs the insurance card for Signa. The problem is that the mother, once she understands that PA1 is asking for the father’s insurance card and not hers, realizes that she can’t provide that information because she doesn’t have a copy of the father’s insurance. In this case, PA1 is left not being able to bill the insurance, and the note unresolved in the system.

There are a series of breakdowns in the activity of resolving unknown patient information. The first is a breakdown in the division of labor between the parents in orchestrating shared knowledge of insurance information. In terms of tool support though, there wasn’t prior support for letting the mother know, before she came to the appointment, that there was even missing information. It appears that someone at the physicians’ offices knew, at least enough to put a note in the electronic file. Proper precautions could have been taken to at least prepare the mother for the lack of insurance information.

Over all, these breakdowns are encountered because of an office staff employee scanning the file and noticing that information in a client file is incorrect. Supporting this kind of scanning is invaluable, and can go far in making sure that other information in a client file is up to date and avert future breakdowns.

Design Implications:

- Support automatic alerts of missing information: email/text/phone call

- Support indicating when a piece of information is known to be incorrect, but not having to resolve the issue at the time.
- Support visual scanning of a patient file to check information in a patient's file.

Med-P15 Observation Notes:

*2010-08-18 1:26PM PC1 is entering information and talks about a wrong address that someone put in that is a joke. I think it is the PC3. PC1 calls PC2 and asks about what address she entered and tells her that she doesn't have to put in a bunch of made up information for an address and can just put in an x. I remember PC1 looking at the computer and when she realizes she has the wrong address concluding that obviously it was because PC3 had put it in there incorrectly. I don't think there was a doubt in her mind that anyone else there would have put in the wrong information. When PC1 gets off the phone she laughs at how silly PC3 was.*

*2010-08-18 2:33PM PC4 picks up the ringing phone. It is another cardio person asking about the phone number for a patient. The cardio person says that the number has expired. PC4 says that she will look it up on his PT sheet. She goes to the blue blinder on the right hand side of the counter -- looking for it. She didn't find it. She gets back on the phone and says that she can't find it. 2:39PM PC2 returns with another stack of files. PC4 asks about the phone number. PC2 says that she made a new file for him and it is in the pace maker pile... PC4 goes over to it and finds the file, finds the new phone number, returns the call of the person who was looking for the phone number. Apparently there isn't an updated phone number.*

*2010-07-01 11:35AM They talk about a folder of a male patient with a female name and the gender being wrong on his chart. I believe this is the man that just left. They said that this happens when they are referred by another office and they generally do not provide gender because it is assumed from the name. Also, other practices do not tell them whether the stress test is a walking one or a medically induced stress test for people that can't walk. PC2 explains that these take different lengths of time and this often causes problems.*

Med-P17 Observation Notes:

*2010-08-19 9:35 Another mother comes to the window and says she needs to check her daughter out. PA1 asks for her date of birth and types it into the system. Three people [items] come up and PA1 says that she needs to look at a note. The patient says that she has two insurances. They try to figure out who are the insurance companies. PA1 explains that on June 29th they were going to get a copy of the insurance - which is what the note says. The patient shows the insurance card. PA1 says that that is an old card, and that this date the place has*

*moved to a signa card. The patient says that is the insurance for the Dad. So she'll have to get it from him. PA1 says that she'll check with PA5 about the insurance. PA1 picks up the phone and says she only has the signa and danaheur card, but she knows it has changed. She says 'oh United, United health care, is that right'. PA1 says for the patient to get back to them as soon as possible. The patient agrees. The patient leaves.*

### **9.3 Proactively Sharing Knowledge Not in Client File (Study 2)**

Observed

- Med-P17 2010-08-19 9:43-9:55AM

Even though P17 has a complete electronic system for their billing and their patient information they still have paper files for all of their patients. This location also has satellite offices across the NRV area and this location is their central location – perhaps why they have so many office staff at this one location. The electronic systems are distributed across all of the offices. The paper files for a patient, after an appointment has been made, will travel to the new location for the appointment.

This breakdown covers how the office proactively lets a satellite office know that they might not have a particular patient's paper file. In this case the doctor has come to PA1's front window, and let her know that there was a patient who was going to come to her window that needed special attention. PA1 makes an appointment at another office, where the office can remove the wart from the patient. PA2 then calls the satellite office know that they might not have the patient paper file for when the patient visits them.

While not a breakdown in the strict sense – the patient's care is handled without a problem – it does highlight how the office acts in a manner to prevent a critical breakdown (i.e., not providing adequate care for the patient). Knowledge of the location of the paper files has to be managed, on top of the care of the patient, and without this knowledge the system breaks down. The electronic system should either adequately support seeing patients across multiple locations, or it should provide a method of accounting for the physical location of the paper file – like a library system.

Design Implications:

- RFID-ing patient files to know their location
- Storing information about the location of paper file in the electronic file

Med-P17 Observation Notes:

*2010-08-19 9:43 A doctor comes down to talk to PA1 about a patient and explains that she is sending them down to her for a reason. I don't catch the reason... 9:48 A patient comes to the window to ask about a particular doctor. The mother needs to make an appointment before her son starts back at school. PA1 looks at the schedule for the doctor. There are three offices she can select from to look at the doctors that are there. PA1 suggested Wednesday, Sept 1st. PA1 is looking at the schedule which has white, red, and gray areas on the calendar. Patient asks for 4 o'clock. <*

*Mother schedules appointment at other location and mother and son leave. > ... 9:55 I can hear PA2 on the phone. She has called someone at another office. It is about a patient who is coming in to have some wart's removed. She says that she just wants to let them know in case they can't find the file there, so not to worry about it. PA2 then puts the file on a stack of patient files on the left hand side of her counter.*

#### **9.4 Recalling Codes (Study 2)**

Observed:

- Med-P17 2010-08-19 10:51AM
- Med-P01 2010-08-20 08:46AM
- Med-P01 2010-08-20 09:15AM

Of the electronic systems I was able to observe, a couple did not possess the easiest interfaces to manage. Much of HCI literature talks about the problems with relying on a user's memory for anachronistic codes, and the medical systems that I was able to observe either did not ascribe to these research findings, or were very old systems. Included below are two pictures. The first is Med-P17's e-MD system used for tracking health and billing information. Even though this interface looks relatively new, it still requires user's to enter memorized codes. The other interface is a picture taken of a DOS based system used in Med-P01's office where the user enters codes into the bottom right blinking cursor.

When PA1 is processing billing information in the eMD system she can see different information about the patient. I was able to observe her entering in the codes for processing payments when I was there. To do this, she sees what patients have been seen, the information for that specific appointment and what was done to the patient, and then the payment information. For PA1 to be able to process the payment with the insurance company, she has to enter the correct codes for the procedures. These codes are then translated into the procedures, and entered into a visible list on the bottom half of the eMD system.

When PA1 is entering the codes, she has to rely on her own memory for entering in the correct procedures. These codes are specific to procedures such as a particular injection, a well visit, sick visits, and many more. When I first arrived, one of the things I was able to observe is PA3 creating a print out of all the new codes for that season's flu shots. When PA1 enters the codes, every time I saw her she was entering them from memory. Her workflow involved typing in a code, hitting enter, and then looking at what was displayed and the corresponding number and cost. The problem and breakdown occurs because PA1 would enter in the incorrect code numerous times, having to go and select, delete, and then re-enter the correct code.

While it was never observed that she entered the incorrect code and left it in the file, she did have to delete incorrectly entered information numerous times that she caught herself. (I didn't have the knowledge to recognize incorrect codes.) The fact that she is having to rely on her memory and then entering incorrect information in the first place is a

breakdown in terms of being able to correctly and easily attach correct information to a patient's file. Not only is this information stored about the patient without any easy way for the patient to review and catch mistakes, but it is hard for PA1, who is highly knowledgeable to be able to associate the correct information with each patient.

Additionally included below are notes from observing Med-P01 where their system was command prompt based. This system is perhaps worse than the one that PA1 used at Med-P17. To be able to access anything in the system the nurses have to enter codes and use the keyboard arrows to move around in the file system. In the examples provided below, PD1 and the supporting nurses rely on PD1's memory of what different codes are. For instance, in the first example PD1 is providing the codes to the nurses, even though the nurses have most of the codes memorized. In this case, the nurse is recalling the special code indicating that her patient had just completed their last visit, thus closing out the electronic file. In a second example from this practice, the nurse cannot recall the code for a specific procedure when she is adding the information to the patient's electronic record. She instead has to ask PD1 for the code to be able to enter it.

In Activity Theory, the objective of this task is to correctly associate a patient's appointment with the codes of the practice. The breakdown occurs when relying on user's memory to enter codes. Because the codes are difficult to remember the user creates mistakes.

Design Implications:

- Use natural language processing to suggest procedures
- Allow for user to enter procedures in multiple ways – such as suggested auto complete
- Allow the patient to review their medical procedures

Med-P17 Observation Notes:

*2010-08-19 10:51 {PA1} pulls up the list, selects the participant she is looking for. If the code/item isn't entered, she deletes the old ones, and enters codes until she gets the right one. Then she saves the item and returns back to the home screen where she pulls up the remaining visits.*

Med-P01 Observation Notes:

*2010-08-20 08:46AM A hygienist comes into the office with a patient file. A patient comes and asks the hygienist if there is anything else, the hygienist tells him that he is fine. The patient leaves. The hygienist then asks PD1 if she gives her the file since he is done. (The files usually go to PD2 to file.) It appears as though this was the patient's last visit. PD1 says that she does give her the file, and asks if the patient has been checked out. The hygienist says no. PD1 gives her the codes for the computer -which must be unusual because the hygienists usually know the code, and the hygienist checks the patient out for the last time, and hands PD1 the folder.*

*2010-08-20 09:15AM A nurse is checking out a patient. She is loudly trying to recall the code for what was done with the patient. When she can't remember, she asks PDI, and PDI shouts out the code, but then checks the code in the folder on her desk. She lets the nurse know that she had it correctly.*

### **9.5 Permanently Missing (or Dead) Client (Study 2)**

Observed

- Med-P17 2010-08-19 11:24AM
- Med-P15 2010-07-01 11:20AM
- Med-P16 2010-09-09 1:20PM
- Med-P17 2010-07-15 9:29AM

Physicians' offices were the place where a patient was discovered to be missing. Childcare centers didn't have this problem because they see the children daily. At a physician's office, if the patient does not show up for appointments, they can become lost in the daily work of the centers. There are times, however, where the center tries to locate a patient to either try or schedule a new appointment or to collect payment, and the patient is not reachable. In these cases, the office has to either turn over the file to a collection agency, or to file the patient as non-active – usually relegated to some location of “purged” files. This is a case where the office maintains sensitive personal information about a client, but the client has severed the relationships – knowingly or unknowingly – between them and the provider.

In the notes listed below, PA3 is working on a child's file. While I was not able to attend to what she was doing to the details I would desire, she had pulled up the child's file on her computer and had the child's physical file in front of her. For approximately 30 minutes she was on the phone on and off writing down notes on a scrap piece of paper trying to locate a child. She finally found that the child she was trying to locate had moved locations and had gone to live with her dad. Based on that information, she was able to pass on relevant medical information (that I was not allowed to write down in my notes), and put the file to be filed. It was my impression that PA3 and PA2 spend a significant portion of their time hunting down clients.

There were other examples where the offices had to spend time tracking down patients. PA4 from Med-P17 spends time with the Medicaid portal for insurance information. This is because even though the patient may have disappeared from their records the insurance company can have updated patient information such as address and phone number.

Both PB1 from Med-P16 and the office ladies from Med-P15 discuss issues where they are trying to determine if their patient's have died. In these two cases it is not that the patient owes them money, but more that they want to know if a person that they have cared for is still alive.

From an Activity Theory perspective, the objective of passing on relevant medical information was hindered by a lack of updated information. This could be attributed to a lack of rules about when and how information should be updated, an unclear division of

labor between who should update the information, or tool support to track and update clients who have moved.

Design Implications:

- Send electronic reminders for patients to update their location information quarterly
- Support patients being able to review their location information moving the labor from the office to the client

Med-P17 Observation Notes:

*2010-08-19 11:24 In the meantime PA2 and PA3 have tracked down someone who has gone to live with her dad and they couldn't get a hold of her or something. They give high fives and go to put the child's file to be filed.*

*2010-07-15 9:29AM PA4 is now telling me about a website that she uses to track Medicaid patients -- it's a newly launched site so it still lacks some functionality. She pulls up a patient with the Medicaid site and goes over some of the information. You can view each patient's primary care provider, name, address, and phone numbers. She says that patients' member IDs can change when they move so sometimes she has to be "like a detective" to find people. Finding their member IDs is important for verifying their insurance eligibility.*

Med-P15 Observation Notes:

*2010-07-01 11:20AM PC3, PC2, and PC1 are talking about calling somebody and that patient may have died. (I'm not sure of any further details of this strange conversation) PC1 takes a page to the fax machine, places it in the machine, and types in a number.*

Med-P16 Observation Notes:

*2010-09-09 1:20PM I asked PB1 about the file she put to the side. She said that it was just the nicest old man. He was coming in for appointments and then he called to say that he was having problems with his prostate. So he stopped coming in. PB1 wanted to call his regular doctor just to make sure that he was doing all right now. She says that she was just being nosy. She says that for some files, she knows right away.*

## **9.6 Missing Documentation to go into a Client File (Study 2)**

Observed

- Med-P17 2010-08-19 11:43AM
- Med-P15 2010-08-26 02:39PM
- Med-P15 2010-08-26 03:58PM
- Med-P15 2010-07-01 10:06AM

Client information that will eventually make it into the client's files comes from numerous locations. For instance, information may come from forms filled out by teachers in rooms, or from nurses entering in information during a patient visit. In the first case covered in the observation notes the information is actually coming from the patient to Med-P17. The patient is sending in a payment through the mail. This information is then entered into the patient's electronic record that is available to everyone in the practice to review. PA1 is the head person who handles payments, so all mail related to making a payment is to come directly to her.

The problem in this situation arises because someone else that is in the practice passes PA1 the mail. In this case someone was supposed to give PA1 the mail, but it went missing for some period of time. I remember PA1 talking about how she said that when she asked this nurse for the mail, the nurse had told her that she didn't have it. But, what PA1 finds out is that the nurse had left them on someone's chair, instead of passing on the mail appropriately.

While the information made it into the patient's files and the payments were processed, the handoff of relevant patient information was diminished. This leaves the possibility for an incomplete patient file, thus affecting the care of the patient. A breakdown occurs in the rules surrounding how mail is to be handled between the office staff: the nurse did not properly hand off mail when she was supposed to. While a technical solution might not solve or mitigate similar breakdowns, presenting visible holes in a patient file to highlight missing information may facilitate changing the rules surrounding passing relevant patient information. In particular, assigning roles to those rules governing the division of labor can make implicit rules explicit.

The second and third examples from Med-P15 illustrate how other information can not make it into the patient file. In the examples from P15 the doctor is reviewing a patient file and sees that there is information missing in the file – annotations from the patient's previous visits, I believe. When the doctor asks PC1, the office administrator, about it, PC1 says that she'll check through her extra annotations to see if anything is there. PC1 has a look, but there is no additional information for that patient. At this point they know that information about the last visit never made it back into the file.

How the breakdown happened in this case is a little elusive. There are many places where an annotation could have gone missing – either the tape never made it to the person who did the annotations, the annotation was never done, the annotation notes were lost, the papers fell out of the file, or many other possible scenarios. The response to this breakdown is to try and reconstruct the missing knowledge and try to extrapolate if the missing previous information will impact health decisions. I believe that more missing annotations would have to be observed before a reaction in the system would be made.

In the second example from Med-P15 the doctor has left for the day without properly completing information for a patient's procedure – that will eventually go in the patient's file and is necessary. PC1 asks the office director what to do, and PC6 knows of a solution. PC6 says to fax the needed information to the hospital for the doctor to fill out

and fax back the next day. In this case, the doctor was able to leave without necessary papers completed to go in the patient's file.

Design implications:

- An electronic system could highlight and ask for further action in reference to missing information.
- An electronic system should support having missing information so that it can be tracked.
- If annotations for a file are missing for an extended period of time this file could be called to the attention of the staff.
- When filling out paper work, highlight information that is missing.

Med-P17 Observation Notes:

*2010-08-19 11:43 Someone comes by and gives PA1 two more pieces of mail. It appears that PA1 was looking for them, because the lady explains where she found them - on a chair in someone's office. PA1 sounds cross about getting them. She slices them open, places them to her right, and then returns to looking at doctor's schedules.*

Med-P15 Observation Notes:

*2010-08-26 2:39PM Dr-PC7 has come in. She tells PC1 that she has left a note, but that she wants to know if the office notes in a particular patient's file are really from a date in March. Maybe the newer notes are lost. PC1 hands more papers (annotations) to Dr-PC7 to verify. PC1 says that she'll look in her little pile and let her know. PC1 goes to her drawer and starts to thumb through... 2:41PM PC1 finishes going through her pile and says that she doesn't not have a note for that date that Dr-PC7 was looking for. She goes to "shout" for Dr-PC7 to tell her. PC3 tells her not to, that she'll get in trouble. PC1 says that is because PC3 throws out accusations, she knows for a fact. PC1 leaves the room. 2:46 PC1 tells Dr-PC7 that there isn't a note for that patient. She adds 'honey' on the end of the sentence, which is the first time I've heard her use a term like that, to soften the bad news to the doctor.*

*2010-08-26 3:58PM Someone has called. There is paperwork that Dr-PC7 was supposed to do, but she didn't answer all of the questions before she left for the day... PC6 has come in to give out the paychecks. PC1 explains the situation to PC6 and asks what she is supposed to do about the papers that Dr-PC7 didn't go through. PC6 explains that the paperwork is supposed to faxed back over and the Doctor will look at it the next time she is in (the hospital?). PC1 gets back on the phone and relays the message.*

*2010-07-01 10:06AM Amanda has some papers at the island and says that she can't find some folders. She looks in a cabinet underneath the counter. She grabs some and Nikki says they might be on the floor behind her.*

## **9.7 Unaware of Client Load (Study 2)**

Observed:

- Med-P17 2010-08-23 9:49AM
- Med-P01 2010-09-01 9:20AM
- Med-P16 2010-08-19 2:30 – 3:19PM

Part of the work of the people in the front office is anticipating the work that needs to be done. Keeping track of these tasks is done through some pretty intuitive visuals – how tall a stack of papers are, how many patients are on the list to be seen that day, etc. A problem arises for these knowledge workers when having to track patient and office progress for what work was done and for when the work that needs to be done is obscured or hidden. For instance, a printed schedule may have patients checked off to show who has been checked in, who is missing and needs to be contacted, and who arrived late. An electronic schedule may only show upcoming and current patients, with little easy tracking of the previous meta-information. What sensitive personal information is displayed about a patient is directly related to how easy it affords managing the necessary work. In reference to privacy and security, it was observed that when these scheduling issues arose, the offices would go into more depth of assessing client information to determine which patient they should cancel on.

In reference to work that was previously completed being obscured, this makes it more difficult for people to attend to what work remains to be complete. In the first observation notes below, PA1 is examining the patients that were seen by the doctor who was on call over the weekend. The electronic system shows her all of the patients who came in for an appointment, but she laments that she cannot see all of the patients who might have called and didn't need an appointment. This information is important for her keeping track of their general patient load – which she is able to keep track of during the normal weekdays by talking with the nurses who triage all of the calls.

Three possible cases result in this breakdown in shared awareness. The first is the electronic system may not support the documentation of seeing a patient by phone. This is a case for a lack of tool support in the objective. The second is that the doctor does not enter this information into the electronic system. This may be the lack of following a rule about documentation, or about a lack of a role to document the phone calls. The third is that the system may not have an easy way to support aggregating and displaying information about visits that were not billable. Again, this is a lack of tool support.

In the second example, the nurses and office staff of Med-P01 manage the scheduling of patients by booking them into particular chairs for time slots. Patient information is then printed out according to the chair on the schedule so that nurses can orient towards who they are supposed to be seeing. A problem arose for the nurse when they realized that someone had been scheduling patients into a 5<sup>th</sup> chair. The office only ever staffs four

chairs, so who would be attending the patient in the 5<sup>th</sup> chair. This is a case where there is a social rule governing the use of the part of the software that schedules the patients, but when it wasn't followed properly resulting in problems in the schedule and also more patient information being displayed and accessed.

In the third example, it is late in the day and the office has realized that they have more work than they can complete within the day. An assistant comes to PB1 and asks her if she can start rescheduling her next couple of appointments. PB1 looks at her schedule and recalls that the patients are both coming from fair distances away and are both probably on their way already. PB1 looks up the patients on her computer and then calls them, only to confirm her suspicion that they are both on their way. There was some discussion about whether one patient would have left already because she is always late. PB1 also expresses doubt as to whether they should even call because they don't want to call someone while they are driving and cause an accident.

These last two cases are ones where time management and scheduling issues have revealed more about patients to determine who to cancel on and how to manage those patients. For instance, one of the patients was scheduled for their procedure because the office had already had to reschedule on them twice, so canceling on this patient was not acceptable. Knowing the patients and the general flow of the schedule allows the place to run smoothly.

#### Design Implications:

- Facilitate in electronic system 'special case' for documenting un-billable phone calls.
- Facilitate information entry after phone weekend phone calls.
- Allow for meta-information about the use of software to be able to be documented – such as not using a 5<sup>th</sup> chair.
- Support orienting towards the schedule

#### Med-P17 Observation Notes:

*2010-08-23 9:49 PA1 talks to PA3 about Dr-PA6 being on call over the weekend. PA1 says that she didn't seem to be swamped with too many patients, but she doesn't know about calls. PA1 has been going over all of the patients who were seen over the weekend and processing their payments. She is only able to see the people who are billable. PA3 & PA1 are talking about PA3's weekend.*

#### Med-P01 Observation Notes:

*2010-09-01 9:20AM Nurse-1 looks at the schedule. Nurse-1 asks PD2 if they are scheduling one into the 5th square now. PD2 says she doesn't think so. There are five chairs in the hygienist's room, but not that many hygienists usually in there. This reference is to asking about if they are going to book more people than they usually have hygienists. Nurse-1 says that she feels like if someone sees that one person does it, they might scheduling them all like that.*

#### Med-P16 Observation Notes:

*2010-08-19 2:30PM Both dental hygienists come in. One asks if someone today can be moved because they are behind schedule. PBI determines that the next patient is coming from Pulaski which is probably too far. The other one comes from Bluefield which is also probably too far. By too far, I mean that they've probably already left their houses so it is hard to ask them to turn around or they might not have their cell phone numbers. They try and figure it out. The dental hygienist comes with the file and is putting it together with all the new papers. PBI calls the next patient who is to arrive and asks if the appointment can be moved. The patient is already on her way. The patient doesn't want to move because she has already been moved once. PBI goes back and tells dental hygienist #2. PBI calls the next patient, and he is also already on his way. 3:19PM 3:19 Assistant-1 comes in and talks about the scheduling problem. She says that for this certain procedure to try and not book them back to back because they take longer. PBI says that they used to schedule an hour and a half for them, but now only an hour. They go through the schedule and look at how it happened, because PBI knows that they take longer than are scheduled. Assitant-1 says that she doesn't necessarily need 1.5 hours, but more than just a maintenance person in between so that she can catch up in between patients. It has to do with the scheduling. PBI can see where they've had to reschedule someone for a reason, which is why the schedule happened the way it did.*

### **9.8 Missing Electronic File (Study 2)**

#### Observed:

- Med-P17 2010-08-23 10:06 - 10:27AM
- Med-P01 2010-08-20 09:43AM
- Med-P15 2010-08-20 1:06PM
- Med-P15 2010-07-01 9:48AM

Of the places we observed they all had both electronic and physical filing systems to keep track of client information. While both systems have different affordances, the electronic system has no knowledge of what is in the paper file, and vice versa. Therefore, in cases when one file, either the electronic or the paper file cannot be found, the practices rely on the other as a back-up, even though it isn't a complete back-up to reconstruct the information. The issue becomes that paper has a clear affordance of being visible in the office and when it is not in the correct location, people can look around the office for places it might be to be found. If an electronic file is not searchable – either because of difficult to spell name – or for other reasons, then the file is for all intents and purposes lost.

Electronic files, from what I can tell, are created when there is a need in the electronic system to keep track of them. For instance, I saw that in Med-P01, the new patient was only entered into the electronic system when it was time for that patient to have their next

appointment scheduled; the patient had already been seen and their paper file was complete. Alternatively, Med-P16 would create the electronic file almost immediately because she wanted to verify if the patient could have their appointments covered by insurance. And, to show another perspective, P15 only created the file when the patient was scheduled to be seen by the doctor.

In the first observation snippet covered in this breakdown, PA1 has realized that there is a patient who was seen over the weekend and she doesn't have any of the patient's information in her electronic record system. The weekend is a time when there isn't any office staff to support the doctors seeing the patients, and so patient care isn't as well documented as during the week. To try and track down the patient's paper file, which PA1 believes must exist somewhere, PA1 calls someone in the office to try and locate the paper file to get that information put into the electronic file.

In this case there is a clear breakdown where the documenting the patient's information had occurred and the electronic file had not been created. This breakdown did not occur because the electronic file had disappeared. It occurred because the normal role, of a person to document new patients, was not available over the weekend (where the weekend functions as a special case). To remedy this situation, PA1 had to leverage the paper file and the work of the people who manage the paper files, that was in an alternative location.

An additional breakdown is provided in the observation notes below where again a new patient has come in, been seen, but when the nurse goes to the electronic system to enter the patient's visit information, the patient is not in the electronic system. While the nurse recognizes that the patient is new, and is able to adapt to the situation and to start a new patient's electronic file, she still went through the system to first examine if the client was in the file system.

In the second to last example, PC1 from Med-P15 has received a phone call from someone who is going to be seen at the practice but has not been seen yet. The patient has a question about the visit, but when PC1 goes to pull up the patient's record, she realizes that they are not in her system. She places the phone on hold, since she can't answer the patient's question any more when it comes to medical information, and waits for a nurse. PC4 takes over the phone call, but only after expressing doubt about whether or not she should talk to the patient about their information – even though they have the information that has been faxed over.

In the last example, PC7 at Med-P15 has said that she cannot find a patient in the electronic system. At this location the patients can be retrieved electronically based off of many identifiers, but the most unique identifier is a patient ID that is assigned. In this case PC7 had tried to look up the patient using other information, but was unable to find the patient. It is only after PC1 recalled the patient number from memory that the patient's electronic file was able to be located.

The more I think about this breakdown, I think it has to do with when a patient becomes a patient for these centers. It appears as though the patient becomes ‘their patient’ when they collect paper about the client and that is made into a file. The electronic file seems to come afterwards, when it is ambiguous as to whether the client should already have an electronic file. For instance, when the electronic system shows that there should be a bill built for a client, but the system does not have the information necessary for billing the patient. It appears that waiting until this point is what causes a breakdown in not being able to access information about the client. There is a lack of a rule about when a patient’s electronic file should be created by these participants, resulting in breakdowns around locating the electronic file.

Design Implications:

- Create places in the system to support missing information, and then notification of that missing information to the appropriate people.
- Create rules surrounding how to handle new patients within special cases such as weekends in the electronic system.

Med-P17 Observation Notes:

*2010-08-23 10:06AM PA1 pulls out a post-it note, and puts it to the right of her mouse pad... 10:14AM PA1 picks up the phone. She asks if someone is there. PA1 says that she is looking for a Baby <name>. It seems like this file can't be found electronically - which is what the post-it note on the side of the mouse pad is about... 10:20AM The person PA1 was trying to reach earlier about the missing information, calls back. PA1 explains again that she can't find the file. This patient was seen over the weekend, but she can't find any of the information. She has a ticket with a payment, but no information about the visit or the patient. PA1 gives the name of the patient and the date, and the payment type. PA1 tells whoever is on the phone to get out of the file because it is locked up. Whoever is on the phone gives PA1 a suggestion... 10:27AM PA1 is looking around the eMD system for invoices that have been built. She clicks on one from Friday that has notes. The notes read that the information about that patient's visit are missing. PA1 closes it. This must be the patient who PA1 was on the phone about earlier.*

Med-P01 Observation Notes:

*2010-08-20 9:43 I'm watching Hygienist-2 and Hygienist-3. They are standing over at the computer kiosk in the hallway. Hygienist-3 has asked for Hygienist-2's help to enter a new patient. They can't figure out whether or not the patient is in the computer with how the patient's name is spelt. PD2 came over and is trying to help them with the computer with entering the computer. With PD2's help they are able to create the new patient in the computer. This is the same patient who PD1 earlier was making the new booklet for.*

Med-P15 Observation Notes:

*2010-08-20 1:06PM ... A patient called and PC1 picked up the phone. She tried to pull up the patient's file on the computer, but they weren't in there. Just because the patient isn't in the computer, though, doesn't mean that they might not be a new patient. So PC1 puts the patient on hold, and asks PC4 or PC2 to take the phone call since they are nurses and can address what sounds like a medical concern. PC4 says that she doesn't know if they should talk to him if he isn't a patient - I assume stating some liability concerns about providing medical advice if the patient hasn't signed a waiver yet. When PC4 gets on the phone, she realizes that this guy went to the ER, and a doctor at the hospital told him that he would have to go to this practice afterwards to be seen again. So PC4 asks the room if they have the records from the soon-to-be patient's doctor and from the ER. That is when PC3 says that she has something from the physician, but not the ER. PC4 gets back on the phone and asks for identifying information [name, DOB, date of the hospital visit] so that she can call and get those records faxed over as well.*

*2010-07-01 9:48AM PC4 is working opposite of PC7 and says out loud that she can't find the patient number of a particular person. PC1 then immediately recites the account number from memory. PC7 comments that she's been working here too long.*

## **9.9 Client Providing Perceived Unnecessary Information (Study 1)**

Interview:

- Parent-P00
- Parent-P11

One parent lamented in her interview that when she was providing information to the childcare about her child, that the only information that was requested was “sterile”. The lack of asking for information about what her daughter likes or does not like made her reflect on the quality of the care that the center would be able to provide for her. While the childcare may gather this information from meetings or from daily interaction, the mother wanted to provide this information up front.

Because it is unclear what information should be included in that file, who accesses, and what it is used for, the parents feel a desire to provide perhaps private information about themselves towards the objective of good care for the child. Clarifying this situation, though, is difficult because there is also an ambiguity about who owns the information, and thus should have control over what is placed in the client's file. The division of labor is clear: clients provide information; centers manage that information. What is not clear though is what information is relevant.

Design Implications:

- Support parents being able to store this information, and then ways to modify it as a child grows.

Parent-P00 Interview Transcript:

*Laurian: ok... so I'm going to ask some questions about the information you provided when you first joined there... so can you think of what information you provided about your child when you first joined?*

*Parent1: yeah there was a whole list of general parents and phone numbers and it was all very sterile and business related... emergency contacts, doctors, insurance... all of that stuff was there... there was no request for "who was your child" so I made your own "who was your child" - "This is <child's name> and this is what she likes and doesn't like" and I was so thrilled when I got my enrollment packet from <Child-P01> that had all the business information and even more pages of "who was your child", "help us get to know your child", "do you have anything to contribute culturally or talent-wise"... none of that was present at this daycare*

Parent-P11 Interview Transcript:

*Participant11: And in addition of that they did not prompt me for but I wanted to provide information on what he likes to do, how to comfort him, things that he enjoys doing. So, they did not have any specific forms for that but I wanted to make sure that they had the information and also the daily schedule. They did not ask for that but I wanted to make sure they had it.*

*Laurian: So, How did you do that?*

*Participant11: I just wrote down in a piece of paper and handed over to a teacher. With that information I went directly to the teacher rather than the administrator and director.*

*Laurian: Why did you give that to the teacher instead of the director?*

*Participant11: I just wanted to go direct to the person that would be caring for him to make sure she has this information. Because I felt it is more important for her to have the information and then emergency contact and health info can be put into the computer by the director but I wanted the teacher directly have that information.*

### **9.10 Client Providing Perceived Unnecessary Information (Study 2)**

Observed:

- Med-P17 2010-08-23 10:19AM
- Med-P01 2010-08-20 09:33AM
- Med-P16 2010-09-07 2:14PM

There were numerous observed instances when patients would hand over information about their medical conditions to the office staff that they would want included in their patient file. This information was usually detailed information about their conditions, ailments, and current prescriptions. From the outside, this practice looks valuable – the patient is providing additional information that may help in their care. What the patient is not thinking about is how they are also passing over private personal information.

In the case listed below in the observation notes, the patient's father is providing information about the birth of the patient to PA1 at Med-P17 that he thinks is relevant to be included in his daughter's file. What PA1 tells me after she has made a copy is that she does not think that this information is particularly useful, but it makes the patient feel better. The office becomes a steward of that private information, even though they do not perceive it to be useful for the care of the patient. This is a case where the rules surrounding who gets to decide what is relevant in a patient's file become obscured. The patient feels that this is relevant information, but the office does not. But, because the information is semi-related to the care of the patient, it is included.

Similar observations were made at Med-P01 with a mother providing a crumpled piece of paper to PD1 about her daughter's health. While an orthodontist may fit within the medical realm, the orthodontist cannot do surgery or prescribe prescriptions. Medical information about her daughter appears a little unnecessary. Similarly, a woman hands over all of her medical conditions, including cancer, to the receptionist for the paper to be copied and put into the patient's file – even though she is just coming in for oral surgery.

The breakdown in this situation relates to a few issues. The first is the relationship between the subject, community, and the rules surrounding what information should be stored in the patient's file (the object).

#### Design Implications:

- Allow for the collection of possibly irrelevant information, but support additional layers of security to access it
- Create sections of a patient's file to support delineation between patient-provided information and physician office-provided information.

#### Med-P17 Observation Notes:

*2010-08-23 10:19AM Another man comes to the window and hands L a piece of paper. PA1 somehow understands that the man wants a checkup for his child. She asks for the birthday, and verifies that it is a 2-month appointment. I ask PA1 what the paper was about. PA1 says that it was the list of vitals, like weight and head circumference, and she doesn't know why he handed it to her, but he did. PA1 says that sometimes patients hand her information like this and she says it makes them feel better to give them a copy, even though she doesn't think that they use them.*

#### Med-P01 Observation Notes:

*2010-08-20 09:33AM A new patient comes up to the front desk. She says that her daughter has an appointment. The mother hands PD1 a piece of paper and asks her if she wants to make a copy of it. It is a description of her daughter's medical condition. The paper is white and a bit crinkled on the edges. Looks like it has been carried around. PD1 makes a copy, puts it in the patient's file, and takes the file through to the Hs room.*

Med-P16 Observation Notes:

*2010-09-07 2:14PM PBI suggests another time, which the woman says that she can do. PBI enters the date into the computer. She then enters it into the paper calendar. PBI then gets a notecard, writes it on it, and hands it to the patient saying that the next appointment will take about an hour. The woman then hands PBI a piece of paper that looks 8x4 inches big, well worn. The patient says that this is a list of all her illnesses. The doctor told her to give it to PBI for her to make a copy. PBI takes it, and makes a copy of it. She writes a note on the copy, and then puts it in the patient file in a particular order - by pulling out papers.*

### **9.11 Disconnect Between Dispersed Patient Information (Study 2)**

Observed

- Med-P17 2010-08-23 10:51 – 10:54AM
- Med-P01 2010-08-20 09:48 – 9:52AM
- Med-P16 2010-09-09 1:20PM
- Med-P17 2010-07-15 10:13AM-10:47AM
- Child-P06 2010-09-09 12:35PM

The practices we were able to observe all except one had paper and electronic records. These record systems had no knowledge of what was in the other, causing a disconnection between people using one system and the other. This can result in a breakdown when information from one system is necessary for the use of the other.

In the first case provided in the observation notes below, a nurse at Med-P17 wants to provide a vaccination to child, but she is unsure about the patient's ability to pay for the vaccination. Payment information is not stored in the paper file, but is instead stored in the electronic system. Given that this patient has signed a waiver saying that she does not have insurance, the nurse has to walk over to PA1's office (away from the care of the patient) to check and see if the patient can pay her bill. This disconnect between electronic and paper information caused a disruption in the care of the patient – who possibly should not have been seen in the first place.

In the second case provided in the observation notes below, the nurse tries to make an appointment in the electronic system for the patient so far in the future that the electronic system does not support. Their paper system, of writing the date of the next patient appointment on the back of the file, does afford making appointments that far ahead of time. The problem arises when it comes time for that patient's appointment and the appointment is in the electronic system, which is what the office relies upon to schedule their daily activities. To prevent a breakdown, PD1, the director of Med-P01, uses a paper based system on her desk of tracking appointments that cannot be put that far ahead of time in the electronic system – noting appropriate patient information.

In the third example PBI from Med-P16 is “purging” files from her shelves. To do this she goes through each file and looks at different aspects of the file to assess whether the patient is “current”. She is trying to determine if it is likely that the patient will return

soon. If the patient is older than seven years (or dead), the patient's paper file is discarded (but their electronic one is not). To make this determination, PB1 looks at the notes on the outside of the file, such as if they are a quarterly patient, she makes a decision. If this information is not enough, she then looks up the patient in their electronic system. The fact that the information about a patient's recent visits and their care plan are not evident in the paper file indicates that there is a disconnection between what information is stored in each patient storage form.

In the third example there is an issue with trying to locate who is paying for what in regards to a particular patient and their insurance at Med-P17. PA4, who is the self proclaimed Medicaid queen of the office, explains prior to the quotation below that the office has trouble with patients listing two insurances as their primary insurance. This results in a problem for the office because they end up covering the difference when they the office gets in trouble. For this patient she is trying to figure out why the payments look funny. From what is presented to her in the electronic system, this looks like a case where the patient is doing something strange with her insurance. After spending 30 minutes on the phone with people at Medicaid, the Medicaid portal, and her electronic file, she is still unable to resolve the issue. It is only have discussing the patient's file with Anita, who has access to a different set of information about the patient, that they are able to resolve the issue. It turns out there was no discrepancy to begin with.

There was only one observation of this similar problem in childcares. Childcares are unusual in this breakdown type because there is so much information about each child dispersed within the environment. There are hubs where certain information is location, but information duplication is more rampant within childcare center than within physician's offices. Within childcares the waitlist was a difficult artifact to keep medicate between the different people who needed to locate it along with the physical and electronic versions. As PE1 from Child-P06 explained, she keeps an electronic version of the waitlist on her computer that has the date and time and pertinent information for the child stored on it. However, she is the only person who is allowed to access her computer. This means that she prints out a version of her electronic one that she then has available in case she is not there. The childcare staff then adds new clients to the physical list at the bottom. They still have difficulties with this problem though between people emailing and communicating with PE1 and then others coming in person to sign up and being on the physical list.

All of these cases illustrate examples where a lack of knowledge about what is in other files results in a breakdown in managing the client's care. The problem is that the different files represent tools for different needs. The breakdowns occur when directed needs are not reflected in the tools or the dispersed files. In order to fully be able to account for all circumstances, records need to at least have knowledge of what is available in other locations to support diverse activities.

#### Design Implications:

- Integration between paper and electronic systems; electronic systems that recognize the use of paper.

- Create a system that pre-notifies if patient has problems with their information before providing care. Support distributing this information from the electronic system to the paper system.

Med-P17 Observation Notes:

*2010-08-23 10:51AM A nurse comes to the window with the patient's file. The nurse said that the patient doesn't have insurance, but she has signed a waiver. The mom said that she paid for the appointment, but the nurse doesn't know if she paid for the vaccine. PA1 takes the file, looks it up on the computer, and then tells the nurse that there is a balance on the account. I think balance means that the mother has money there, not owes money. The nurse says that she'll send the patient back to her before she leaves. PA1 hands back the file and the nurse leaves... 10:54AM A woman comes to the window. It looks like this is the woman that the nurse was talking about. PA1 explains the payment of the shots and the signing of the waiver. They conclude that the woman doesn't owe anything. The woman leaves.*

*2010-07-15 10:13AM Speaking of which, PA7 comes up to PA4 to discuss an issue where a patient is making payments to their office while on Medicaid.*

*"PA4, I need you to pull up a patient. This women is making payments and she has Medicaid" ... PA4 is now using the Medicaid web portal again to look up this patient. She works diligently for the next few minutes with this site. She types in a name or number several times but every time she presses search nothing comes up. 10:19AM PA4 makes a call: "Can I speak to one of your eligibility workers for a patient <patient name>? I'm having some trouble verifying..." She tells the person on the line (from social services) that there's a problem with a patient she's looking up. The patient's page is showing two different primary care providers which is something she's never seen before. PA4 continues the conversation for several minutes and is on hold for much of this time. While on hold she turns to me and tells me that not even she knows what's going on with this patient. 10:28AM. The call finally ends and she tries to type an id number into the portal once again. After a few tries she seems to give up as the search isn't finding anyone. She silently works with this website for a few more minutes without saying anything to me. 10:47AM PA4 tells me that over talking with PA7 she has cleared up the problem with the Medicaid patient. She tells me that the patient was only paying during April so there were actually never any real problems to begin with. Unfortunately this whole situation took 30 minutes even though there was never a discrepancy to begin with.*

Med-P01 Observation Notes:

*2010-08-20 09:48AM Hyginist-1 is still working with the mom, and tries to enter the date in December for the appointment, but the appointment*

*can't be entered into the computer that far in the future. Hyginist-1 tells PD1 about it, but that she is going to write the date on the folder - which appears to be the only place it is going to be noted... 9:52 Hyginist-1 asks PD1 about when an appointment for December can be made in the system and pulls out a sticky note for her self to remember to make it later. PD1 says that if she gives her the file, she'll do it later today. Hyginist-1 writes a note on the file and puts it in PD1's pile.*

**Med-P16 Observation Notes:**

*2010-09-09 1:20PM I ask PBI a bunch of questions... So, I asked her why she was looking on the computer as well. She said that she keeps track in both places, but that it isn't so obvious on the paper files. There is a little note on the outside corner that says something like quarterly, and that means that the patient should be coming every three months. She says that the doctor likes to see some patients for a period of time after their surgery to do the cleanings here just to make sure that the surgery is healing well for about a year or so. Then the doctor will discharge the patient to their regular doctor and he has a large procedure where he writes a letter to their normal dentist. So PBI will look at the file, but she will also look them up in the computer because the computer has more information than just this little hand written note on the corner of the file. I'm not sure what extra information the computer provides - I know that it provides a list of the last time they came in.*

**Child-P06 Observation Notes:**

*2010-09-09 12:35PM PE1 returns back to typing and the teacher who she was talking to continues to use the computer that is in the reception area. I ask L what she is doing now. She has pulled out the wait list binder from the top of her shelves in her office. She says that she is updating the information from an email that she got, which doesn't have all the information, but has enough. She is telling a lot of information to me right now. 1, they are getting a new website and have a new web designer, she wants to be emailed with people from the website. 2. The waitlist. She used to have a system set up so that she could see the files on the other computer in the reception area. But, she got a new computer and she can't figure out how to set that up again. So instead she has a binder that she uses and puts things in there as they show up from email or people stopping by. This is very important for them, because people from this international center will come in upset because someone got called before them, and they insist that they came in earlier that same day to be put on the wait list. So she puts it on paper, which everyone can access, and then she will enter the paper in manually into a computer file. They update the file occasionally when there has been a lot of movement.*

**9.12 Disclosing Patient Information (Study 2)**

Observed:

- Med-P01 2010-08-20 08:56AM
- Med-P15 2010-08-18 03:11PM
- Med-P15 2010-08-26 12:43PM
- Med-P15 2010-08-26 02:31PM
- Med-P01 2010-06-07 9:20AM
- Med-P17 2010-07-15 11:50AM

It was generally observed that the locations we visited were aware they were stewarding sensitive personal information, and took precautions where they saw appropriate, but there were still times when an office employee would overly disclose personal information either by accident or without knowledge that what they were doing was wrong.

In the first case listed in the observation notes, PD1 from Med-P01 has created a booklet for a new patient, and she needs the patients name and address. Because the file for this patient has already been taken through to the hygienist's room, PD1 does not have access to that patient's personal information to look up. (I believe that the patient also did not have an electronic file as well.) Instead, she walks over to patient room, which I had recently walked past and saw about 10 people sitting in, and asks the patient for their name and address. The information is verbally disclosed loud enough that everyone in the room and I am able to hear.

While I have no way of knowing whether there was any harm from this incident, it highlights a clear lack of standardized rules surrounding what is considered private information, and what is not. In this case, the patient's name and address is not considered private by the office, while it might be considered by private by HIPAA.

In the second and third examples, PC3 shouts out a patient's full name in Med-P15 even though there is a known rule surrounding disclosing identifying information. In the first case PC3, though, did not know about the rule at the time. The other office ladies and since told her that disclosing a patient's full name is against HIPAA and she knows not to do that again. This is a case where a breakdown had been resolved by educating PC3. In the alternative case PC3 accidentally says the wrong patient name, in what I believe to be a case where she wants to feel like she knows all of the patients and guesses at who she thinks is the next patient on the schedule. While this kind of breakdown will be elevated as PC3 gets to know more patients, she should also be educated about saying the incorrect patient name in a way that does not result in a disclosure.

In the third example, people at Med-P15 realize that the fax number that they have for faxing a patient prescription is incorrect. They had been faxing the patient's prescription to a different fax machine number that was active, because they received fax confirmations, but was not the correct number. They don't check where they information may have gone to, they only update their records so that they do not fax the incorrect number a third time. This example illustrates a time where information is disclosed outside of the practice, and one where nothing is done to either let the patient know about the breach or make sure that the information was shredded. There is clearly a lack of

rules surrounding how to appropriately recover from this privacy breach, thus resulting in the base case of zero response.

Design Implications:

- Visually indicate to the office staff what is private versus not private in a patient's file. Maybe shades of color could be used to indicate the degree of privacy.
- Support something like digital certificates between locations to verify they are who they say they are.

Med-P01 Observation Notes:

*2010-08-20 08:56AM PD1 takes one of the sheets that were printed out over to the window and asks the patient who is waiting what her name and address is. The patient provides it verbally. PD1 writes the information onto the sheet for the booklet.*

*2010-06-07 9:20AM PD3 walks into the x-ray room and back into the office. She sits at the desk by the door at the DOS computer.... PD3 asks PD1 to read somebody's phone number to her because she cannot read the numbers. Then she dials the number.*

Med-P15 Observation Notes:

*2010-08-18 3:11PM ... PC3 points out a sticky note with a patient's name that PC4 left out. PC4 got rid of the paper. They then talk about HIPPA violations and patient identifying information. PC3 shouted out a patient's name in front of another the other day. PC3 says that she didn't know that you are allowed to say a patient's names as long as you don't say first and last name at the same time...*

*2010-08-26 2:31PM PC3 says the wrong name to the patient when he says he is here for a stress test. He says sure to the name. PC3 goes to look at the files that are stacked to the right of the in-patient window, realizes her mistake, and says the right name. He says that was right enough. He asks that if she kills him if he gets a refund as PC3 runs his credit card. This was a bit of a joke, but there is some truth to it.*

*2010-08-26 12:43PM PC3 is on the phone with the pharmacy for the patient who said that the prescription was not received. PC3 gives the date and time of the original fax and says that she just faxed it again. PC3 tells PC2. PC2 says to confirm the fax number. PC2 rolls over and drops a file off on the island opened to where PC2 was writing in the note. PC3 finds out that the fax number was incorrect. So what happened here is that PC3 figured out that they had a wrong fax number and had now incorrectly faxed a patient prescription to the wrong location twice.*

Med-P17 Observation Notes:

*2010-07-15 11:50AM PA8 told Red or Purple that this lady is going to yell at her because she did not have her sign a release form.*

### **9.13 Auditing and Preparing for Office's Incorrect Patient Information (Study 1)**

Interview:

- Med-P05
- Med-P13

PH1 from Med-P05 explains that they use the audit system to verify when changes were made to a patient's file to support a kind of us versus them mentality. She says that patients can call or show up saying that there is an error, and the system is used to show when a change was made to support the office. In a second example PN1 from Med-P13 does not use individual passwords but she does have people sign their name when they make a change to an electronic file so that she can verify when a mistake has been made.

These two examples demonstrate how directors report only using the auditing (that is not actually supported by the electronic record but through a social policy for how to use the software) to prepare for any mistakes that may happen in the future. Whether it is preparing for patients saying that they did or did not have an appointment, by making a notation of who accessed and changed a record, the director is capable of back tracking.

Design Implication:

- Support methods for directors to be able to track who has made changes to the record/schedule

Med-P05 Interview Transcript:

*Laura: Is there an audit trail?*

*PH1: Yes and we use that a lot. Last week I had a patient show up at the front desk for an appointment and I had to tell her I didn't have her for an appointment at all, and she was getting all huffy about it so I pulled it up on the computer. With the audit trail then I could say that on June 21<sup>st</sup> at 3:53 am someone left a message on our answering machine and cancelled. So we use that a lot. I don't use it too often, but I do occasionally to find out who did what on what computer, so like if a transaction got deleted and nobody knows anything about it. We do that quite a bit.*

Med-P13 Interview Transcript:

*Laura: Is there an audit trail?*

*PN1: As far as does it record everything they do? Yes. It shows the name at the bottom.*

*Laura: Do you ever use that?*

*PN1: Yeah actually, because there will be times that something was changed and I'll look like I don't remember doing that, who did that?*

*PN2: Why was this patient scheduled here?*

*PN1: Yeah who scheduled them for 5 minutes before we close? That kind of thing*

### **9.14 Auditing and Preparing for Office's Incorrect Patient Information (Study 2)**

Observed

- Med-P01 2010-08-20 09:28AM
- Med-P01 2010-06-07 11:21AM
- Med-P17 2010-08-23 11:11AM

It was observed that the office staff in different locations would review information in a patient's file to make sure that it was correct – especially in circumstances when the information was coming from people who were outside the central office. For instance, Med-P01, as covered in the two observation notes below, would review all of the information coming in from satellite offices because there were too many times when work was being done incorrectly. PA1 at Med-P17 also processes all of the payments so that they can be done at one central location without any mistakes. The ladies at Med-P15 constantly examine files that are coming in and track information to make sure that the information that is correct.

The purpose of this auditing is to track information and to make sure that it is correct. For instance, PA1 at Med-P17 explained that after faxing over a letter to a school to get a child out of class, she will keep a copy of the file and the confirmation of the fax and put it into the patient file, just in case the school calls to say that they did not get the file. (Med-P17 2010-08-23 11:11 “PA1 explains that the template it used a lot in strep season. A copy of the fax is kept in their files in case the school tries to say that it was never sent. PA1 has printed out the letter to the school and it is on the left-hand side of her desk.”) This kind of file keeping and auditing is done, mostly because the offices recognize that mistakes can be made, and when they do, their work may be audited. The process of pushing papers to support later auditing, creates a lot of work, but is important for spotting where breakdowns happened.

This kind of visible paper stack is obscured in electronic systems, and makes them unusable for distributed offices like Med-P01's office. Because PD1 had such trouble tracking down payments in their electronic system, she mandated that she be only one to process payments.

Design Implications:

- Support visualization of relevant information for tracking errors in patient files—when information was sent, who sent it, etc.

Med-P01 Observation Notes:

*2010-08-20 09:28AM PD1 has a patient file, pulls out the x-rays and moves them towards the back of the file. PD1 explains that she does all the financials for all three offices. It used to be that the other two offices*

*would try and post payments, but now they don't because it was taking her too much time to go in and fix their work.*

*2010-06-07 11:21AM PD1 tells me that she's the bookkeeper for all of the offices since other people make too many mistakes. This leads me to believe that she had people taking care of bookkeeping before but it ended badly.*

### **9.15 Knowing a Patient's Private Circumstances (Study 2)**

Observed

- Med-P01 2010-08-20 09:48AM
- Med-P01 2010-06-07 10:32AM
- Med-P15 2010-08-18 02:24PM
- Med-P15 2010-08-20 01:42PM
- Med-P16 2010-09-09 01:03PM

Particularly when dealing with children, there was more information that was known about the child that was not necessarily relevant to the care of the child. And, in order to care for the child, this additional information had to be accounted for. For instance, when dealing with children, there were times when parents were divorced and had to both manage the care of that child. In order to schedule and organize the care for the child, knowledge the child's family circumstances dictated how well the physician would be able to administer care. This is a case where what is perceived as unnecessary private information actually attributes to the care of the child.

The breakdown occurs because managing this kind of meta-information about a patient currently does not exist in the either record keeping system (though, it is easier to account for in the paper system, and other participants have discussed how they do that in the interviews.) Because this information is considered secondary, it is not managed and thus results in a breakdown in terms of managing the care of the patient.

In the observation notes below, a mother and father are divorced, but have two children who are receiving care at the office. When the mother tries to schedule an appointment at Med-P01 for her daughter to next be seen, she realizes that her husband will have custody of the children, thus she cannot schedule the appointment. While this appears that this is merely an issue of coordinating care for the parents, the parents are not talking to each other. This then becomes an issue of the practice becoming an in-between communication channel between the two parents.

Similarly, at Med-P01 a father has called to cancel the work for his child. He tells the office that he will no longer pay for his child's orthodontic work because his son has been kicked out of the house to encourage him to make something for himself. While this creates extra work for the office, it is the child who is the client and not the parent who is paying for the care.

Understanding the social dynamics between the patient and their family is important for managing the care of that person. Breakdowns occur when there is not an easy way for the practice to access and reinterpret this information within new contexts. Because Med-P01 is a small location and they are familiar with their patients, tracking the social information is easier than if the practice had ten times the number of patients.

In the example from Med-P15 PC4 and PC1 are talking about a patient who PC4 had attended to earlier. PC4 says that the patient came in because he says that he is having chest pains. Based off of the test results, though, it looks like the problems are not related to his heart or anything that they can do something about at that physician's office. In discussing this with the patient PC4 suggested to him that perhaps his chest pains were from anxiety. This is when the patient started to get over excited and PC4 and PC1 speculate it is because his wife said the same thing to him. This kind of information, about the personality of client affects the care of the patient, and thus should go into a patient's file. However, it is not.

In a third example, a patient who is requesting a prescription has called Med-P15. PC1 was the one who handled the phone call and wrote a note about taking to the doctor about the prescription. The doctor was not in the office that day, which is why she wrote a note. When PC4 looks over PC1's notes from the morning, she sees this note and tells PC1 that this patient is a prescription seeker, and not really sick. Whether this is true or not, it is information that PC1 did not know about the patient nor was it made apparent in looking up the patient.

In the last example, from Med-P16, everyone in the office knows the personal circumstances of one patient: that she met a man; that she was trying to sell her house; but that the house is no longer on the market. This information, while having nothing to do with the care of the patient, is about understanding how to care for the client. If the patient sells her house, she will have to leave the practice, thus affecting whether she is a client any longer. It is stored in the collective knowledge of the practice, and not in her file, so that they can better manage her as a client.

Design Implications:

- Support storing meta-information about a patient that can be easily recalled prior to next appointment.

Med-P01 Observation Notes:

*2010-08-20 09:48AM ... Hygienist-1 is still working with the mom, and tries to enter the date in December for the appointment, but the appointment can't be entered into the computer that far in the future... So what has happened here is that a mother of two children who are being seen at this practice. The daughter has finished her appointment. The mother, who is divorced from the father, comes into the middle of the room where there is an empty desk with the hygienist to make the next appointment. When the appointment time is suggested, the mother says that she doesn't know if that appointment is possible, because that is when*

*the father has the children, and she doesn't know his schedule. There is a lot of back and forth, where the Mom tries to make it their problem with communicating with the father to tell him the appointment. When the mother adds that she needs to make an appointment for her son as well, it becomes really complicated. This is when PDI gets involved because, as she tells me later, she has had experience with these kinds of circumstances. PDI suggests making an appointment for when the mother has the children again. This, though, isn't until December. But, without giving the mother too much time to say that won't work for her, they set up the appointments - with difficulties entering the appointment so far ahead of time, and suggest that she leaves. After they leave PDI tells me that she has seen many cases where parents aren't talking to each other, and have to coordinate the care of the children. It can become problematic because they feel like they are messengers between the two parents. 09:51AM Hygienist-1 and PDI confirm that the problem was separated parents who do not want to talk to each other. The dad has accepted a job in Utah and one of the daughters is going with him, but the other one is staying with her mom.*

*2010-06-07 10:32AM Somebody's dad called and said not to make any more impressions or retainers because he is not going to pay for them. PDI tells us that his son isn't living at home now because the father kicked him out. The father was trying to encourage the son to get a job, but it was not working. Now the father is trying to get him to go into the service, like his brother did.*

Med-P15 Observation Notes:

*2010-08-18 2:24PM In whispered voices PC4 talks to PC1 about a recent patient who was talking about inconclusive evidence about chest pains. It seems that she asked the patient if his chest pains could be anxiety related, which got the patient worked up. PC4 did an impression of his indignant raised voice.... in whispers. PC4 concluded that the patient's wife must have been accusing him of faking his chest pains. PC4 then left to see a patient.*

*2010-08-20 1:42PM PC4 tells PC1 that the person who called earlier this morning is a drug seeker and the doctor isn't seeing him anymore. The patient is on some medication to help with the seeking drugs.*

Med-P16 Observation Notes:

*2010-09-09 1:03PM The doctor, Nurse-2, and PB2 are all huddled around PBI's desk talking. A patient comes in, and they talk to her about how her husband has decided to move to the area and she isn't moving. I'm not sure why they make such a big deal about this patient, but she is fairly young, so that might be it. It seems like everyone in the office knew her bidness - that she was moving to be with a man. The woman says that she*

*couldn't sell her house, so he decided to move here so that they could be together. N2 tells the patient that she is ready for her and the patient follows N2 to the back room.*

### **9.16 Lack of Password Use (Study 1)**

Interview:

- Med-P01
- Med-P07

As explained in the interview notes from Med-P01, the reason she says that they do not use passwords is because “They can access anything. That’s their job.” The office director sees having unlimited access to patient information as a requisite to the role of being an employee. Either client privacy is not a concern, or, more likely, understanding the social norms surrounding accessing patient information is expected to be in the role of an employee. Similarly, Med-P07 explains that her system does not even provide multiple logins for each person, so there is no point to use them.

This kind of breakdown reflects a place where there is either a lack of a tool to support password use, or there are other rules that support security and privacy that do not involve security and privacy.

Design Implications:

- Support passwords for offices that want to use them.
- Support other social methods of managing the security of the information.

Med-P01 Interview Transcript:

*Laura: What about who can access what information? There are 7 people who work here... can they all access all that information?*

*PD1: Yeah. Um hmm. Patient information. Scheduling.*

*Laurian: What kind of information might they not be allowed to access?*

*PD1: They can access anything. That’s their job.*

Med-P07 Interview Transcript:

*Laura: Okay are there privacy policies built into the software? Does every person have to log in to it?*

*PA3: There’s no login once it’s in the mainframe computer. They know all our licensing and information they have it right there, so once we’re in there we can access everything from all the computers in the office.*

### **9.17 Lack of Password Use (Study 2)**

Observed

- Med-P01 2010-08-20 9:48AM
- Med-P01 2010-06-07 9:50AM
- Med-P16 2010-07-13 1:42PM

Interview:

- Med-P19

There were only three times in all hours of observation that a log-in to any electronic system was observed. The first time was at Med-P17 where PA4 and PA7 shared passwords to get into the hospital record system. The second time was when the office staff logged out and logged back in between checking email (Med-P14 2010-07-06 11:50 am “PR1 is still gone and PR2 is still typing and clicking in MediaDent. She quickly checks her hotmail and re-launches MediaDent and logs into it with her user ID and password”). Instead computers were used as communal tools, like a kiosk, that anyone could use for the work they needed to accomplish.

This breakdown occurs because there is private information stored in the file system that is being left unsecure. A rule surrounding logging into the electronic system simply does not exist, or if it does, it is not followed. In another case, there are passwords, but these passwords are shared and not unique to individual users, therefore again disregarding the purpose of internal passwords. Because there is not a rule surrounding or mandating password use, logging in and out of an electronic system is redundant – as noticed at Med-P16. This may be because the rules surrounding appropriate use account for security and privacy in different ways. For instance, as was noted on 2010-06-07 at Med-P01, there is always someone in the office able to observe who is accessing what information. This kind of social accounting is one method that the practice used to manage the security of the patient information.

As shown in the observation notes of Child-P06, passwords are not how information is kept secure. When a teacher needs a password to the computer, she merely shouts asking for it. The password is then shouted back in response. While passwords may be present, they are not actually used to keep information secure from those who exist within the centers.

Design Implications:

- Support other types of logging of people updating and accessing client files.

Med-P01 Observation Notes:

*2010-08-20 09:48AM So far I haven't seen everyone log into any computer. It seems like they are all logged into the same system with no password.*

*2010-06-07 9:50AM It's important to note that there is virtually no security when it comes to the files and the terminal systems. There doesn't seem to be a login since people just leave the screen open once they're done using it. The files are accessible by anyone, including the assistants. With that said, however, there's always someone in the administrative office so anyone sneaking in unnoticed is virtually impossible.*

Med-P16 Observation Notes:

*2010-0-13 1:42PM PBI brings a paper over and punches it on the counter next to me. She leaves her office with it, leaving her computer unlocked.*

Med-P19 Interview Transcript:

*Aubrey: Oh, okay. For the EMR, is there a login for each individual user?*

*PSI: Mhm. Yes it is.*

*Aubrey: But each user has the same*

*PSI: Password.*

*Aubrey: They have the same password and they have the same access within the system.*

*PSI: Yes. Yes that's correct.*

### **9.18 Difficulty Locating Client File (Study 1)**

Interview:

- Child-P01
- Child-P08

There were cases where childcare directors reported difficulty locating a child's file. Childcare centers are audited to make sure that they have all of the files that they are supposed to have and all of the documentation is up to date for each child. During these audits directors can become aware that their files are not present. Other cases that directors reported of noticing when their files were not in the correct location is when they look up a child's file to place new information inside of it, or when the waitlist is being accessed.

Design Implications:

- Support knowing where a physical file is such as using RFID.

Child-P01 Interview Transcript:

*Stacy: "Are there any problems, or is there a need to keep the two synced up so that they have the same exact information in them? The physical and the digital?"*

*Interviewee: "A lot of it's the same, it may be that the format is different between the way it reads in the database versus how it came off the website, but we do keep it, merely for the backtrack experience of you know 'oh, wow, their file got lost in the database somehow, I have to go back and hand search 5 years of waiting list to find their information and then track it--notations are made on the hard copy you know, I often initial and it says 'date entered 10/13/09,' so that there's the hard copy there."*

Child-P08 Interview Transcript:

*Tom: so you mentioned there is no difference of information... if she needed to pull a child file she wouldn't go through you or anything..?*

*Interviewee: no, she would just pull it...she might have to help me find it sometimes...if we've pulled one - and that's a problem we have, you know, we'll pull a file to look up somebody's phone number and the file won't get put back and then it gets buried on the desk*

### ***9.19 Difficulty Locating Client File (Study 2)***

Observed:

- Med-P01 2010-08-20 10:25AM
- Med-P01 2010-06-07 9:20AM
- Med-P01 2010-06-07 10:55AM
- Med-P15 2010-08-18 1:46PM
- Med-P15 2010-08-18 2:13PM
- Med-P15 2010-08-18 3:30PM
- Med-P15 2010-08-20 2:18PM
- Med-P15 2010-08-20 2:46PM
- Med-P16 2010-08-19 3:18PM
- Med-P16 2010-09-07 2:33PM
- Med-P15 2010-07-01 9:30AM
- Med-P15 2010-07-01 10:05AM
- Med-P15 2010-07-01 11:05AM
- Med-P16 2010-07-13 1:42PM

A patient's unique identifier is their name. When a patient's file needs to be located, it is primarily by their name – either typing the start of their name into the system, or scanning the paper files which are sorted alphabetically. The task of finding one file within many paper files was made easier by having different stacks and knowing which stack to look at (e.g., active, current, inactive, purged).

It was observed that three offices had fourteen separate difficulties locating a patient's physical file when name is the primary key. This is because physical files can get misplaced and misfiled. It is also because a patient's name can be hard to spell, or because of cultural differences between switching the ordering of the first and last name.

In the observation notes below, PD1, the office manager for Med-P01, who has relative knowledge of all patients in the office, cannot find a patient who she knew was coming in because of the unusual spelling of his name. Also at Med-P01 there was an instance of a file not being in the stack it should be in, and similarly, another where one person in the office repeatedly does not re-file folders correctly. Med-P15, there are three instances within two hours where a significant portion of time is allocated to finding a patient file that is not in the location that it should be in. The next day there are two additional instances where there was difficulty in locating a patient file, and a case where all locations have been searched and two patient records were not found. In Med-P16, where there was the smallest number of files, still had two instances where a paper file could not be located.

These instances of not being able to find a patient's file is more than just about the fact that there are too many files for the staff to search through. This is about the office managing their workflow – that there are charts to be signed off on, or waiting for faxes to come in, or for faxes to go out, or other circumstances. When a file can't be found, it means that at some point in the workflow the file is not where it should be. The lack of

known location lends itself to calling attention to cases that are unusual and thus needs attending to.

Design implications:

- Support knowledge of the location of a physical file, such as an RFID
- Support secondary keys for a client
- Support a visual indicator for where a file is within an office workflow.

Med-P01 Observation Notes:

*2010-08-20 10:25AM A patient and his mom comes to the waiting/checkout area. PD1 teases the young man about spelling his own name correctly, which is what was causing the confusion earlier with finding his file. He laughs. H-in-training comes to the computer and finds an appointment for the patient. What has happened here is that there is a young man who has finished his appointment. He has an unusual spelling of his name. PD1 had problems finding his file based on how he spells his name, and was teasing him about it.*

*2010-06-07 9:20AM PD3 just got off the phone from setting a time for two girls. They are sisters and neither one came to the appointment, but only one was in the follow up stack for some reason. PD3 asked PD1 where she should look for the missing file and PD1 pointed toward some files near the door.*

*2010-07-06 10:55PM PD1 mentioned a librarian working for them did not know the alphabet so she would sometimes file patients by their first name or put them in the wrong spot. If she could not find a patient's folder then she would skip them and move on to something else.*

Med-P15 Observation Notes:

*2010-08-18 1:46PM A nurse, I think PC4, is looking for a file and can't find it. PC3 helps her look for it. She starts to look around the different stacks in the room. And then PC1, when she has a moment to attend to what they are looking for, says that it is under the front chair area where there is a stack of files that aren't labeled yet. The nurse looks and sure enough, there it is.*

*2010-08-18 2:13PM PC2 asks PC4 if she has seen Patient-B's file and PC4 says no, and PC2 says that she can't find it. It looks like there is paper work needing filing that she moves to the bottom of the pack to find later.*

*2010-08-18 3:30PM PC4 asks PC1 about a patient with the last name griffin. PC1 says what her real name is. PC1 says that something came in earlier but that her chart is like 3 inches thick and it might be in the*

*<special machine> files. PC2 comes in. Now all three are looking for her file.*

*2010-08-20 2:18PM PC2 returns. She can't find two patients, but she found the rest she was looking for. PC4 asks for the patient's name who has arrived and it is given to her. PC4 has the white book and is paging through it looking for the patient's sheet but cant find it. PC1 thanks PC2 for bringing up the files she wrote down for PC2 to bring up from the dungeon.*

*2010-08-20 2:46PM PC4 comes in and is looking for a chart. They guess that another person has taken the chart. PC1 says that the other person shouldn't have taken it because she isn't allowed to. They guess that maybe PC2 took it... PC4 didn't find the file but goes and sits down next to the copier.*

*2010-07-01 9:30AM PC2 says, "Why cant I find Paul's folder?" after browsing the wall behind me.*

*2010-07-01 10:05AM PC2 has some papers at the island and says that she can't find some folders. She looks in a cabinet underneath the counter. She grabs some and PC1 says they might be on the floor behind her.*

*2010-07-01 11:05AM PC2 has papers in hand and is looking for a folder from the shelves. She does not find it, but takes a stack off the island and leaves (took to nurse's station).*

#### Med-P16 Observation Notes:

*2010-08-19 3:18PM PBI explains to me the naming scheme for the folders - the first two letters of the patient's last name. She says that they do this for misfiling - to be able to find lost files. Today she couldn't find a file. It was because the patient was Asian and transposed the name. She found the file, but only because she thought of that.*

*2010-09-07 2:33PM PBI asks me to move so that she can get a file. I do, and she looks around for a bit and then finds it about 2 cubbies over (20 files) saying that it was misfiled.*

*2010-07-13 1:42 PBI gets behind me to get a file and says, "There it is. It was misfiled." She takes it to her desk, opens it, writes on it, and types into her calculator.*

### **9.20 Inappropriate Disclosure of Incorrect Patient Information (Study 2)**

#### Observed:

- Med-P01 2010-09-01 08:55 – 09:26AM
- Med-P14 2010-07-06 11:53AM (Tom + Aubrey)

In larger practices familiarity with every patient is not possible. Instead, a larger reliance on patient charts and documented information is necessary for the continuous care of patients. This can mean that for some health care professionals the differences between patients can become blurred, and mistakes can be made when associating one patient's information with another.

In the observation notes below from Med-P01 a mistake in a letter sent by the practice has been called to the attention of a client. A letter has been sent to a client about some necessary procedure, but instead of the patient's name being in the letter, a different patient's name was included. The office then goes through a process of correcting the mistake, drafting a new letter, and mailing the letter. The doctor, who does some dictation to PD1, the office manager, is very upset by the mistake made by PD2, the other office staff employee. A reference is made by him about the fact that this is a legal document, implying that this is information that is supposed to be protected. The observation shows how the patient's information is then transcribed in the wrong letter to correct it, a new draft of the letter is composed, post-it notes holding dictations are used, and many people in the office discuss the issue.

A breakdown occurred in the disassociation of the letter from the patient's information. It is easy to imagine a scenario where PD2, the letter drafter, was told to write a letter but then became confused about which patient she was to draft it from – say another file was placed on top of the one she was working on, or she stepped away from her desk and became confused about what she was looking at to reference the patient's name. Because there is a dislocation of patient information to drafted letter, it allows for a breakdown in transcribing the correct private information. For this reason, it is easy to imagine a system where the patient's information is automatically included in different document templates, and then also backward associated so that the letter that was sent is included in the patient file. This would allow for easy recovery when mistakes are made, but would also reduce any chance of breakdown by not allowing for different patient information to be included in other documents.

In a similar example, a doctor is sitting with a patient and looking at the schedule for her next appointment. The doctor sees that someone else though, has been scheduled for that time, and sends the patient to the front desk to clear up the issue. In talking with the office staff, it is revealed that the patient's husband has been scheduled for that time when she is the one who should be scheduled. This instance would not be a breakdown had the office not disclosed the husband's name to the patient. While the patient probably knew her husband was a client at the location, that information is still considered private. Again, this case illustrates how additional information about the client, such as their next appointment time, is disassociated from the client's record, making accidents and disclosures easier to happen.

#### Design Implications:

- Support linking electronic templates to patient information, and vice versa.

Med-P01 Observation Notes:

*2010-09-01 8:55AM PD1 gets a stamp and puts it on another piece of paper that was on her desk. PD1 takes a red pen and looks like she initials and signs the paper... PD1 takes the paper she was just stamping and signing and paper clips it to the top of the patient file she was working on. She takes the patient's file and puts it on the stack for the doctor to look at... 9:09AM The doctor comes into the room to talk about a patient. [The Doctor and PD1] are talking hushed like and facing away from me. He says does she, [PD2], realize that this is a legal document, and holds up a paper that is paper clipped to the back of a file. I can see something crossed out on it. The phone trills, PD1 picks up, and the doctor is reading what looks like a letter. PD2 comes back in, and the doctor tells her that this letter is going to have to be re-typed. He talks with PD1 and says that there is going to have to be sentence added to the top that says that this letter is written in correction because they have the wrong name in the letter. 9:12AM ... The doctor starts to dictate a sentence to PD1 which she is writing down, "This letter is sent to correct our typo mistake the first paragraph..." ... The doctor dictates to put in parenthesis "(M\*\*\*\* not Z\*\*\*\*\*)". He says to retype the letter and file it. Doctor leaves. PD2 comes back into the room after developing film... PD1 says to PD2 that she still has the letter on file, right? (Making it a question.) PD2 says that she does, and pulls up the letter on her laptop computer. 9:16AM PD2 asks if she can have the letter and leans over their desks to get the letter with the things crossed out from PD1 (patient file is still attached). PD1 walks over and has what the doctor wants said on a pink sticky note and it is put on top of the old draft of the letter. PD1 explains it to her, and PD2 looks busy typing in the changes to the letter... 9:20AM I can hear the doctor telling PD1 that he wants to read the letter before it goes out and he doesn't want her to sign it (which makes me assume she was asking him if she should sign it.) 9:26AM The doctor comes in and says to PD1 that he wants to put in an apology in there as well at the end. PD1 goes over to the letter that is still waiting on PD2's desk and makes a note. When PD2 comes back into the room... PD1 explains the note.*

Med-P14 Observation Notes:

*Tom: 2010-07-06 11:53AM A female patient comes up to schedule a new appointment while expressing a bit of confusion. She thought she already had an appointment scheduled but Dr-PR3 told her that he didn't see it. PR2 looks into it and discovers that a "Robert" is scheduled on the 12th. The patient says "Robert!? that's [supposed to be] me!" PR2 admits to putting the wrong person into the system and goes on to correct it.*

*Aubrey: The woman in the green and white shirt comes out and Dr. Meyers is behind her. He says to schedule her as soon as possible. She thought she had an appointment, but Dr-PR3 couldn't find it in the system. PR2 finds it after several seconds and says that for some reason it was put*

*under the lady's husband's name. They decide that the appointment must be for her since her husband has never been here.*

### **9.21 Office Staff Hiding Information (Study 2)**

Observed

- Med-P01 2010-09-01 11:25AM
- Child-P01 2010-09-02 2:06PM

Paper affords being hidden. It can be placed in the back of a file, it can be folded and stored under another object, and it can be hidden in obscure locations. Given the plethora of information being stored in the locations being studied, there were times when participants were observed hiding information – in particular, information that was stored on paper.

For instance, in the first example, PD2, an office staff employee from P01 starts to hide a sheet of paper that stores her information. Earlier in the day two nurses had an audible fight in the next room. Throughout the morning, both PD2 and the other office staff employee, PD1, go and talk to both women to get ‘both sides of the story.’ After PD2 returns from talking to one of the women, she goes over to PD1’s desk, grabs her time card, and decides to hide it. She says that she doesn’t want other people ‘knowing how much she makes’, but really this is an issue about how open the location is, and how she desires privacy over her own information.

A breakdown occurs between the subject, community, and a tension between the rules of openness and the objective of privacy. Because the subject is part of the community that values openness and open communication, when the subject expresses the objective of privacy, she engages in nefarious behaviors that are abject to the community norms. This kind of breakdown cannot be rectified unless the community norm of openness is addressed to respect places of privacy.

Design Implications:

- Facilitate places and spaces for personal privacy

Med-P01 Observation Notes:

*2010-09-01 11:25AM PD2 goes over to PD1's desk and gets one of those sheets I saw Nurse-3 writing on earlier. I ask her what they are, and she says her timecard. She says that she is going to hide hers. I ask her why, and she says that people like to come and know everyone's business. She doesn't mind people knowing what hours she works, but she doesn't want people knowing how much she makes. She puts the card on a shelf, and then looks around for a possible better place.*

Child-P01 Observation Notes:

*2010-09-02 2:06PM PE1 explains the privacy issue. She says that what they talk about in the meetings and what goes in the book is private. They aren't 'bashing' people, they are here to help others. So don't keep the*

*notebooks out where people can see them - don't leave them where parents might see them. Try to keep them in private places.*

## **9.22 Patient Confusion Over Procedure (Study 2)**

Observed

- Med-P15 2010-08-18 1:31PM
- Med-P15 2010-08-20 1:06PM

There is a lot of mystery surrounding medical procedures for lay people. Procedures are covered in confusing language usually with doctors speaking too quickly to understand what is happening. Add to that the fact that patients are usually anxious, or generally not in a state to hear relevant information about a medical procedure. For this reason alone, patients can sometimes become confused about their medical procedures and request additional information.

In the case provided below from Med-P15, a patient has called because she is confused about an up coming stress test. She is asking about if she needs to stay up the entire night before the stress test. This confuses PC1, the office manager, because it is not the office's procedure to have the patient be sleep deprived before a stress test. She asks PC2, a nurse, to handle the patient's call. Yet, even in talking with PC2, PC2 is unable to figure out why the patient believes she has to stay up the night before. Instead PC2 tells the patient information about the procedure, and what she will need to do – constantly reiterating for the patient not to worry about the procedure.

In a second example from Med-P15, a soon-to-be patient calls and asks about what is supposed to be done next. He believes that the doctor who talked to him at the hospital, where he was seen about his heart, is now the doctor at this practice and he is not sure about what to do. He talks to PE1 about the upcoming appointment, but she cannot tell him much about his condition because she does not have his full record. The lack of information on both sides of this conversation is the cause for the breakdown.

The breakdown occurs here between the patient, and the objective of understanding protocol for up coming procedures. The patient is told information about the procedure, one can assume, in a manner that was either incorrect or the patient interpreted incorrectly. Language, in this case, which is used as the tool to communicate the objective, is what has failed to support the objective. Asking the patient to review their personalized health plan, which explains the procedure in reference to their care, could avert this breakdown. Or, for patients without internet access, having an electronic system call the patient and repeat information about the procedure to the patient. This would allow for information about the procedure to be repeated at a time with less cognitive stress, while also supporting the objective.

Design Implications:

- Support multiple ways for patients to revisit information about their up coming procedures.

Med-P15 Observation Notes:

*2010-08-18 1:31PM A patient has called and sounds confused because she thinks she is going to do a stress test on Monday. PC1 had picked up the phone (which is typical) and tried to listen to the patient's concern. But when they, PC1 and PC2, looked in the computer, the patient coming in is listed as a new patient and not for a stress test. PC1 has asked PC2 to handle the call... In this instance, PC1 has to move away from the computer so that PC2 can look at the electronic file. PC2 looks up the patient's information, spelled out loud by PC1, and then PC2 picks up the phone and talks to the patient about the appointment. 1:33PM ... PC2 clarifies to the patient on the phone that the test is not a stress test and that the patient was last at this location in 2006. This conversation was a lot of back and forth, until PC2 is able to calm this patient down. I think the confusion was that the patient believed that she had to stay up all night for a stress test. Since this is a heart doctor, they do tests on patients to test the strength of the patient's heart. But this test doesn't require the patient to stay up all night. PC2 hangs up the phone. She talks to PC1 about why the patient thinks she has to stay up all night. They don't really know why the patient thought that she had to stay up. They conclude that it might be that the patient is stressed about the stress test that she cannot sleep. PC2 returns to putting the paper work that the doctor has signed/filled out into the patients' files.*

*2010-08-20 1:06PM PC4 gets on the phone, she realizes that his guy went to the ER, and a doctor as the hospital told him that he would have to go to this practice afterwards to be seen again. When [PC4] gets (Kaelber et al.) information she tries to get [the patient] off of the phone, but the patient seems to be continuing to talk. The patient is confused about whether the doctor he saw in the hospital was the doctor at this practice. I'm guessing that the doctors here sometimes do rotations or are called in for emergencies at the hospital. After PC4 has all of the information she needs, as she continues to talk to the person on the phone the eye rolling was pretty huge. She was clearly making fun of this confused patient.*

### **9.23 Missing Client Information (Study 1)**

Observed:

- Child-P03 2009-10-21 10:05AM -11:25AM

In the example below a teacher talks to PP3 at Child-P03 about a child's medication in her classroom that does not have the child's name on it. The basic issue is that there is not proper documentation for administering the medication or proper documentation to demonstrate that a doctor prescribed it. The teacher does not feel comfortable administering the medicine. PP3 then goes through the procedure of contacting the parent to determine if the medicine was prescribed, and to let the parent know that they will need the proper documentation to proceed.

This breakdown occurs because the rule or policy was not made clear to the parent. In this case for medication to be applied to a child the childcare requires a prescription. The bottle of medication looks like it should require a prescription, but they are not sure. This ambiguity is the result of missing information.

Design Implications:

- Create specific rules for medicine.

Child-P03 Observation Notes:

*2009-10-21 10:05AM A teacher comes in with a small bottle of medicine. She says the bottle only has the child's name in it, but there is no information of the medication. The child has diarrhea and the mother told that medication is for healing diaper PC5. The teacher is not very inclined in using a medication without knowing the name or type of the medicine. PP3 asks the teacher about the parent's number. She is going to contact the parent and query about the medication. The medications are kept in a box in the director's office. Every medication has information listed with it like the child's name, reason for taking the medication, expiration date, name of the medication. 10:50AM Some parents call and talks to PP3 about having the child's name in the medication. The parent is not comfortable with the child's name showing in the medication. PP3 explains that each medication should have a prescription and the child's name must be labeled to it. Later I came to know that the medication is kept in the directors' office, in a locked box and each medication has 4 pieces of information labeled on it: name of the child, name of the medication, reason of taking it, the expiration date of the medication. 11:25AM Call from a parent. PP2 passes this to PP3. This is about the medication that does not have the medication name in it. Earlier some teacher showed concern over this issue. PP3 was asking the parents' number to the teacher. I guess the teacher gave this number to PP3 later since she didn't give it to PP3 when I was there. Maybe PP3 could not get hold of the parent at that time. I hear PP3 telling the parent that bottle does not have any name on it. It has to have a name of what type of medication it is. In this case, it only has the child's name in it. They can only use it for a short time. The parent must provide the details of the medicine. She hangs up a little later.*

## **9.24 Missing Client Information (Study 2)**

Observed:

- Med-P15 2010-08-18 2:27PM

Similar to 'Missing Documentation to go into a Client File,' there are times when a client has been seen or talked to, but the most recent information is not translated into the patient's file – in any form, or even in a meaningful form. This can happen for a multitude of reasons such the staff were interrupted and forgot, it was not deemed as important at the time, or others.

In the example covered in the observation notes below PC2 from Med-P15 is calling patients about their faxed in Coumadin reports to tell people that they either need to stay on the same dose, or to go higher or lower. PC2 calls one patient to tell her to no longer take the medicine, only to find out that he patient is already off of the medicine. She says that she knew that, but that she or something else forgot to mark a note in the patient's file.

When information is missing from a patient file, this can result in a breakdown that affects the care of the client. In the simplest sense, this can be that medical prescriptions/advice/procedures are ordered based on inadequate information. Or, in the social sense, the relationship can be affected. In the example above from Med-P15, the trust between the client and the office is affected because there is an appearance of inadequate maintenance of their records. In this case, the activity of updating a patient on their medication revealed a breakdown in the activity of maintaining patient relationship. At the time of this observation, little was observed to repair that breakdown.

Design Implications:

- Reveal missing information when a patient is called to update their record – such as when going over a reading.
- Highlight areas that may change for a patient between previous check-in and current check-in for the staff to review.

Med-P15 Observation Notes:

*2010-08-18 2:27PM PC2 calls a patient to change a dose on a medication. The patient says that she is no longer on that medicine. PC2 finishes the conversation and says that she forgot as soon as she was off the phone that the patient was no longer on that medicine. She makes a note on a sheet. She then calls two more patients to tell them to stay on the same dose of Coumadin. PC3 takes notes on what looks like a log sheet. She types on the computer, writes on the paper.*

## **9.25 HIPAA Violations (Study 2)**

Observed:

- Med-P15 2010-08-18 2:53PM
- Med-P15 2010-08-18 3:11PM
- Med-P16 2010-08-19 3:12PM
- Med-P17 2010-07-15 10:07AM

Medical offices are guided by regulations, such as HIPAA, that stipulate how patient information is to be managed. While no two locations appropriated HIPAA the same way, the locations were still cognizant that the regulation was in place. However, three locations had instances where they knew that they were not HIPAA compliant, yet they did not respond to alleviate the breakdown.

In cases where HIPAA is not being followed, it is a breakdown between the HIPAA rule, and the office as the subject within the larger community of physicians' offices in the United States of America. The activity of managing patient information, as managed by the HIPAA rule, results in a breakdown when interacting with the local activity of individual practice. These two activities result in a breakdown where HIPAA violations made be voiced by people in the practice, but little action is taken.

In the first example, PC4 from Med-P15, is talking with other office staff about how the files are stored is against HIPAA. HIPAA states that patient files must have data "safeguards" and as such be stored in filing cabinets that can be locked or in electronic systems with password protection (<http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>). Med-P15, however, keeps patient files in a multitude of places that are not HIPAA compliant – on top of filing cabinets, stacked on top of wheeled carts, in a huge stack behind the door. PC4 laments that even though she told the office director that they are not HIPAA compliant, nothing is done to rectify the issue.

Later in that same day of observation PC4 from Med-P15 talks again about how the office is not HIPAA compliant. In neither of these two instances is action made to rectify the situation, and I recall PC4 being called "Little Miss HIPPA." In the second example, PC3 points out to PC4 that she wrote a patient's name on a scrap piece of paper. This privacy breach leads to the discussion about how PC3 shouted out a patient's name in the waiting room. PC3 makes many comments about how she did not, but now she is a bit more educated. So PC4 then asks her if she knew that it is against HIPAA policy to even give an identifying description of the patient. (Upon checking if this is true, it appears that it could be in the section of HIPAA on "de-identifying health information".)

In an example from another office, Med-P16, an auto mechanic called saying that he had a man who was there that said that his wife was at the oral surgeons. But, the man could not remember which one she was at, and he needed to get a hold of her for some reason, I think it was because his car broke down. The auto mechanic tried calling this office, and sure enough his wife was being seen there at that current moment. At the end of this story, Nurse-3 mentions that PB1 verifying that the patient was at their office is a HIPAA violation. The doctor then makes a joke about how Nurse-3 is "little Miss HIPAA Compliant." She responds by saying that they do not know that the husband and wife were broken up and he was going to go on a murdering spree – to highlight that the HIPAA rule might have a good application. Instead of a discussion about how to handle the situation in the future, they then discuss murdering sprees and the group disperses.

In a last example someone has asked for a copy of a client's records. She does not know what to do because there is not a medical release that is signed, but the person needs the records. This case illustrates that the HIPAA policy is salient, but that there are times when how to apply it still are not clear.

All of these instances highlight how rules that are external, like HIPAA, are enforced through their adoption into community rules. Without that adoption, enforcing the

HIPAA rule is brushed off and ignored. For software, this creates a strange design decision to either support the community practice of supporting patient privacy, or supporting how HIPAA says that information should be managed. If the system does not support the work that people want to do, it will not be used, and if it does the system could be liable for patient information disclosure. This is situation where what 'is' and 'ought' are conflated.

From an Activity Theory analysis, the issue here is an overarching US-centric activity of protecting client information through HIPAA is in conflict with the local activities of providing client care. The local interests override the national regulations in the enactment of managing client information thus resulting in a breakdown where rules are broken.

#### Design Implications:

- Visually identify/highlight information in a patient's file that can be used to identify the patient, and then also information that cannot be used. This highlighting could fade when viewing patient information for longer than say 5 seconds so as not to be annoying.
- Create standard rules surrounding how to handle patient information

#### Med-P15 Observation Notes:

*2010-08-18 2:53PM PC4 talks about the filing cabinets about files falling on your head and it hurts. They are talking about how the files are currently used are a violation. PC4 says that she mentioned it to PC6 about the problems with the filing system. PC6 agreed that there is a problem. PC2 agrees that they hurt and they make a big mess when they fall - which means that they papers must be going places. She talks about the big piles of the pace maker files. How they have them is a violation. But that it takes two people to get a file down from the bottom of the pile.*

*2010-08-18 3:11 ... PC3 points out a sticky note with a patient's name that PC4 left out. PC4 got rid of the paper. They then talk about HIPPA violations and patient identifying information. PC3 shouted out a patient's name in front of another the other day. PC3 says that she didn't know that you are allowed to say a patient's names as long as you don't say first and last name at the same time. And then PC4 says that she did know, but did they know that you aren't allowed to use information that could identify the patient. For instance, when she had a 500 lb legless patient she couldn't use that information to describe the patient.*

#### Med-P16 Observation Notes:

*2010-08-19 3:12PM Dr-PB3 comes in and PB1 talks about a phone call earlier. It was another office. It was a man who was looking for his wife and he thought that she was at the dentist. And so the place figured that the wife might be here. And sure enough the wife was at this location. So PB1 said that she would pass on the message to the wife - which was that*

*he was at the garage across the street and needed picking up. The doctor said that that was good. But Nurse-3 said that was against HIPAA. The doctor jokes that Nurse-3 is all HIPAA compliant - he acts like he doesn't take it very seriously. She says, "Well, that is about privacy, what if he was an estranged spouse looking for his wife to kill her." And then they talk about people going on murdering sprees for a second. There isn't a conclusion on whether or not PBI did the right thing.*

Med-P17 Observation Notes:

*2010-07-15 10:07AM PA1 talks through the window about how to print past medical records and what to do without a release form, since that's technically a HIPAA violation.*

### **9.26 Task Interruption Disrupts Managing Client Information (Study 1)**

Observed:

- Child-P01 2009-10-13 5:30PM

In the below example, PT1 from Child-P01 laments that she forgot to make a note of whether or not a form was sent home for a parent to fill out. She says she forgot because she was interrupted, but the fact that she was speaking made the fact that she was interrupted so often appear to be a problem.

These types of breakdowns occur because activities have different levels of immediacy. Additionally, the role of the director means that her tasks have different priority due to the division of labor. Given these facts, interruptions are part of the job, and allowing for differing activities is required in this design space.

Design Implications:

- Support context switching in tasks to protect against interruptions.

Child-P01 Observation Notes:

*2009-10-13 5:30PM I half wonder if PT1 is trying to keep me quiet when she shares that she "hate[s] when [she] get[s] interrupted because [she] forget[s] to write down that [she] sent a note home." She's referring to her immunization checklists depicted in Figure 5, a stack of which are under her pen-in-hand (ObservationP1Oct13.mp3, [01:26:43.26]).  
"That's the only hard part, is that I get work done, but I get distracted."*

### **9.27 Task Interruption Disrupts Managing Client Information (Study 2)**

Observed:

- Med-P15 2010-08-18 2:52PM
- Med-P15 2010-08-18 3:36PM
- Med-P15 2010-08-26 12:32PM

Errors can happen when office staff employees are interrupted. Part of the reason that this can happen is because offices can be hectic places with numerous interruptions – the

phone going off, new patient's coming in, doctors requesting help. Office staff employees have to be able to drop what they are working on at that moment and attend to the business at hand to return to their task later. This also means that office staff employees multitask while waiting for other tasks to be complete. For instance, in the first observation notes below, PC4 from Med-P15 was waiting for a fax to finish. Once the fax came in, she put the fax in the place in the file that she had prepared, but forgot to add all the remaining papers that she took out to prep the file.

One negative affordance that paper has is that it can be accidentally misplaced. It is hard for electronic files to fall and displace information. Or, as in the first observation notes below, when information is pulled out of a file so that new information can be placed in the middle of the file, papers with client information are left out. This information, if not noticed quickly could become disassociated with the patient's file and result in lost patient information or a privacy violation.

In the second example, from the same office, PC4 is writing notes about a patient on another sheet of paper. This task is interrupted, and when she returns to finish writing her notes, the file has been returned and she cannot recall whom she was writing the information about. It is only after five minutes that she is able to recall whom she was writing about, and writes down the name so that she can go back and pull the file later after she is done with her current new task.

In a third example, PC3 is handling making copies of patient information such as driver's license. In the middle of making copies she is interrupted to do another task, and forgets her place, and almost does not make correct copies. While having a less busy workplace can alleviate this kind of breakdown, this is not really a workable solution. Instead, the technology should adapt for the situation, and support taking the patient's IDs, scanning them, and not relying on humans.

This kind of breakdown is one of the primary issues relating to the busy office locations. While paper systems are better than electronic ones, neither support office staff being interrupted or multitasking in a meaningful way. That results in mistakes, breakdowns, and undesired privacy disclosures.

#### Design Implications:

- Keep a running stack of multitasked work that can be returned to. For example, if a patient's record is closed to pull up another one, before closing a flag could be marked to return to the work later.
- Maintain the context of the work done by that patient. For instance, when the user returns to looking at that patient, show a quick video of what work was done on that patient to help with recalling context.

#### Med-P15 Observation Notes:

*2010-08-18 2:52 PC1 asks PC4 if she forgot something. PC4 looks and sees that she left about 20 pieces of paper out of a file. PC4 says that she was waiting for the fax confirmation. They laughed about it.*

*2010-08-18 3:36PM PC4 turns to PC1 and says that she cannot remember the patient who she is writing her notes on. The file has already been filed and she can't find it. She is going to call the office and see if they remember when she is done... 3:41 PC4 remembers the name she was looking for. She writes it down on a pad of paper that is next to the stack of files she has.*

*2010-08-26 12:32PM ...The man in the waiting room comes back to the window. PC3 runs to try and get his IDs copied. She takes the papers from the man and hands him back his ID. In this instance, she was quite literally frantically running between the two. She doesn't multi-task well, and sometimes in the middle of doing one thing she would forget why she was doing it. In this case, I remember her taking the patient's ID, and then trying to do something else why it was copying, and then running back to the patient at the window to hand him back his IDs only to remember that she needed to make a copy of the back of the card as well - so she ran back and make another copy.*

## **9.28 Knowing Patients Personally (Study 2)**

Observed

- Med-P15 2010-08-20 1:00PM

Med-P15 is one of the physicians' offices that knew more of their patients on a first name basis and was constantly reviewing and recalling patient information. With that fact set aside, there are going to be people at every physician's office where the staff know the patients personally. This can mean that there are issues of boundaries between what is private and what should not be shared between the patient and the office staff that will be crossed.

For example, in the observation notes below, PC2 from Med-P15 calls a patient because she has received test results back. PC2 justifies to me why this is appropriate by relaying the story where she helped the family with an important personal medical crisis. PC2 was not observed to be taking this special care of other patients (not saying that she should or should not).

What is important is that when PC2 sees this information the privacy norms and rules surrounding appropriate disclosure become obscured. The relationships of clients to office staff are not clearly outlined in the rules surrounding the roles that people are playing in this relationship. Breakdowns surrounding appropriate disclosure of private information can happen. For instance, she was easy with telling me about the particularities of the boyfriends suicide attempt simply because the person related to the patient's test results came in.

Design Implications:

- Support documenting special relationships between office staff and clients.

Med-P15 Observation Notes:

*2010-08-20 1:00PM PC2 tells us she is going to call her neighbor who lives down the road from her about some results that came in. PC2 tells me why she is close to them. PC2 tells me that the person she is going to call is married with a wife. Their daughter had a boyfriend. The boyfriend tried to kill himself. PC2 was there to help, and so that is why she is closer.*

### **9.29 Difficulties Between External Offices Sharing Patient Information (Study 2)**

Observed

- Med-P15 2010-08-20 1:10PM
- Med-P15 2010-08-20 2:47PM
- Med-P15 2010-07-01 11:35AM

Physicians' offices have to work in an interconnected community for the patient's care. This includes pharmacies, referring doctors, labs, and others. In order to properly provide adequate care for the patient, information must be shared between the locations (usually sent by fax). Breakdowns can happen, though, in sharing the patient's sensitive information between two locations.

For example, in the observation notes from Med-P15, Wal-mart, which is one of the places in town where prescriptions can be refilled, has told the patient that they have tried faxing Med-P15 two times for a prescription refill. The patient, who is upset over why their prescription is not refilled, contacts Med-P15 and talks with PC4. PC4 says that she'll try to figure out what is going on. She gets off the phone, and while on hold the fax for the medicine comes in. PC4 then spends significant amount of time explaining to the patient that it was not their fault, and then being short with Wal-mart for lying to the patient.

In a second example, PC4 from Med-P15 discusses with PC1 a phone call that she had earlier. A person from another office called as the office's representative to serve as a liaison between them and this other office. PC4 was saying how nice that job would be and how useful it would be for patients. She talked about how there are a couple of practices where they just do not like the office staff, and having a liaison would help with sharing patient information between the two locations.

These examples illustrate places where the relationship between the office and the larger medical community are engaged in the activity of patient care. A breakdown occurs when the rules surrounding who is accountable for what patient information, and how to share or pass that information within and among the community are obscure or not followed. While an easy solution for this problem is some automated electronic sharing system, which would not impact the social nature of sharing information or contacting each other when current tools are non-operational.

#### Design Implications:

- Set up information sharing relationships to access patient information
- Support and document difficulties in sharing information for the patient to see.

#### Med-P15 Observation Notes:

*2010-08-20 1:10PM PC1 explains that the person on the phone says that Wal-mart has faxed a prescription twice -- but it isn't coming here. PC4 picks up the phone and tells the patient that the refill request is going somewhere else but not to the practice. PC4 says that she's happy to call the pharmacy to make sure that they have the right number. PC4 asks for the medicine that needs to be refilled... 1:15 PC4 calls the pharmacy and jokes that she is going to just read a number off of a card. In this case she is lamenting about how she is being paid to just read their fax number to a pharmacy receptionist. PC1 takes a print out off of the printer and hands it to PC4. Turns out it was the prescription refill that came in. PC4 laments that she hates that places can't admit that they didn't do it right. Looks like Wal-mart just didn't fax it over until the patient complained. 1:25PM PC4 is on the phone. She called the patient back to tell them that it was Wal-mart's fault and not theirs and that Wal-mart was lying. This is important to PC4, because she doesn't want her patients to think that they are incompetent.*

*2010-08-20 2:47 They are talking about what it would be like to be a liaison for a company. They say that it might be nice to have a face for a company instead of having office staff pissy at another office's staff. PC4 says that they have a bad relationship with another office where they are constantly being mean to each other. It would be better if there was a liaison... She then talks about how it would be great of this office who they hate would have a liaison, because it would probably help the patients instead of them spatting at each other.*

*2010-07-01 11:35AM They talk about a folder of a male patient with a female name and the gender being wrong on his chart. I believe this is the man that just left. They said that this happens when they are referred by another office and they generally do not provide gender because it is assumed from the name. Also, other practices do not tell them whether the stress test is a walking one or a medically induced stress test for people that can't walk. PC2 explains that these take different lengths of time and this often causes problems.*

### **9.30 Office Relationships Affecting Client Care (Study 1)**

#### Observed:

- Child-P03 2009-10-15 4:07PM

In an example from Child-P03, there were issues of gossiping and talking about colleagues “behind their backs”. This was such a problem that PP1, the director of the

center, was writing a citation in the employee's file and was going to bring up the general issue at the next staff meeting.

Design Implications:

- Support documenting that does not require staff to talk to each other.

Child-P03 Observation Notes:

*2009-10-13 4:07PM PPI is typing on the laptop. I have seen her typing something whenever she gets a little time today. I ask her what she is doing. She tells me that she is entering some information about an incident. This is a report and this will be presented in a meeting that is coming next week. The incident is about two teachers, where a teacher said something about another teacher without knowing that the other teacher was also present there. This happened in a bus and the other teacher was a little behind the person who was doing all the talking. The other teacher, who listened to everything the teacher said, notified PPI of this incident. When PPI asked the teacher who was doing the talking, she accepted the fact that she did talk a little about that other teacher but also denied saying most of the things, which were provided by the complaining teacher. There are some teachers in the center who said earlier that this particular teacher talks behind their back but this time someone actually listened and complained. There would be meeting next Monday about this incident. And PPI says that some action would be taken on this teacher in that meeting.*

### **9.31 Office Relationships Affecting Client Care (Study 2)**

Observed:

- Med-P01 2010-09-01 10:05AM
- Med-P15 2010-08-20 01:18PM
- Med-P15 2010-08-20 01:21PM
- Med-P15 2010-08-20 02:47PM
- Med-P17 2010-08-23 09:23AM
- Med-P15 2010-07-01 11:58AM
- Child-P06 2010-09-15 11:06AM

While there is not much that technology can do to solve this kind of breakdown, it is one where patient care and information management is going to be affected. It involves the interpersonal relationships between people, and how they are working together. For instance, if two people do not like each other, they may delay in passing on information, or try to use an intermediary to share information.

There were numerous examples of interpersonal relationship problems observed. The first happened between two nurses at Med-P01 where they had a fight that I was not able to hear the details of. It resulted in the two nurses going to two separate locations in the office and avoiding each other for the remaining time that I was there. Both PD1 and PD2, who work in the front office, left at separate times to go and talk to both parties to

get their “side of the argument”. Neither woman who argued was seen to talk to each other again for the observation period.

In Med-P15 there is one person, PC3, who the rest of the practice regards are highly incompetent. When the doctor left for the weekend, he left instructions for how to manage his patients with PC3, who is his assistant. One of those instructions involved how to manage patient prescriptions while he is out of town – saying that no prescriptions should be sent out. PC4 is annoyed because she feels like PC3, instead of the doctor, is stopping her from being able to do the work she knows how to do a lot better than PC3. Her resentment of working with PC3 stops her from working quickly with PC3.

In another example from Med-P15, PC2 talks about how the office does a lot of teasing of each other. For instance, PC4 teased PC5 about his sheep, everyone generally teases PC3 about being innocent, and PC2 is teased about patients. This kind of teasing was intrinsic to this office. However, PC2 explained that sometimes people get upset at the teasing and will spend a couple of days not talking to one another.

In a last related case from this office, PC4 from Med-P15 also talks about how her practice has difficulty working with other physicians’ offices. PC4 says that if there was an intermediary between the two practices that the relationship would be better and the outcome would be better for the patient.

In another example, a nurse at Med-P17 is overhead talking about how everyone at that practice is going to patient with one another because they are understaffed. It appears as though when people start snapping at each other, the work moves at a slower pace.

In an example from childcares, there was an issue about a man being hired at Child-P06. One man being hired became a large topic of conversation whenever he came in to interview, when he accepted the job, and when he came in to fill out paperwork. In discussion about him PE1, the director of the center, mentioned that there were two men who worked at the center over the summer. She says that even though those men are no longer working at the center they are still causing trouble between people who work there. From the tone of her voice, I assumed this to be romantic troubles rather than something like embezzlement.

#### Design Implications:

- Have any electronic system support being an information channel between two people in a disagreement.

#### Med-P01 Observation Notes:

*2010-09-01 10:05AM I can hear people arguing in the other room. PD2 says that this is the way it is when they hire people right out of high school, you get drama. I says that it doesn't make much sense to me, I can't understand it. She says that it is just the way it is. ... I can hear in the other room someone telling another person that they are all drama. Then someone turns on a vacuum and I can't hear anything. PD1 returns*

*to the room. Office Assistant-3 comes into the room and asks if they heard the argument. PD2 laughs.*

Med-P15 Observation Notes:

*2010-08-20 1:18 PC4 has a patient's file and is writing down notes as she is talking about this subject. PC4 asks PC1 what PC3 asked her to do with the faxed prescriptions. PC4 says that PC3 worked something out with Dr-PC8. PC4 says that she doesn't get told the private discussions between the doctor and PC3. That she is \*just\* the nurse - this is said sarcastically... PC4 is upset because Dr-PC8 will tell PC3 things that won't be told to her. This is particularly frustrating to PC4 because she believes PC3 to be, among other things, highly incompetent.*

*2010-08-20 1:21PM A patient has called in asking for a prescription refill on a medicine. PC3 has said that the doctor told them not to do any prescription when he is not there. PC4 wasn't told this, and she normally has the authority to call in prescription refills. So PC4 leaves the room to go talk to PC3, who has her own office space in the second story of the building. I assume this is to try and figure out whether PC3 thinks the doctor was talking about all prescriptions or just new prescriptions.*

*2010-08-20 2:47 They are talking about what it would be like to be a liaison for a company. They say that it might be nice to have a face for a company instead of having office staff pissy at another office's staff. PC4 says that they have a bad relationship with another office where they are constantly being mean to each other. It would be better if there was a liaison... She then talks about how it would be great of this office who they hate would have a liaison, because it would probably help the patients instead of them spatting at each other.*

*2010-07-01 11:58AM PC2 says they have a lot of fun but sometimes they make somebody mad and they won't talk for a day or two. PC1 puts papers in a folder (has to take some pages out to put them one in). PC1 and PC2 are both on the phone.*

Med-P17 Observation Notes:

*2010-08-23 9:23AM A nurse in the background says that they are short staffed this morning and they are going to be nicer to the nurses and everyone is going to use teamwork and not bite people's heads off.*

Child-P06 Observation Notes:

*2010-09-15 11:06 PE2 leaves. There is discussion between me, the teacher who came in earlier and does the wal-mart shopping, and PE1 about how he is going to be trouble. PE1 says that they've had two men work here, and they've been gone since July, and they are still causing troubles. She says that one of them isn't even on the same continent and he*

*is causing troubles. She thought that women were gossipy, but these guys caused problems. She said that she thinks that it is good that PE2 has a girlfriend, because it will be easier for him. The two that were here over the summer both didn't have girlfriends, which she think is what caused problems.*

### **9.32 Staff Catching Incorrect Medical Procedure (Study 2)**

Observed:

- Med-P15 2010-08-20 1:55 – 2:42PM
- Med-P15 2010-08-26 2:15PM

The staff in centers were observed to review client information. In physicians' offices staff were observed to review a patients file when it was first pulled, when the patient called for an appointment, when the patient called with a question, when a fax came in for a patient's file, and when the file came back into the office after the patient had been seen by the doctor. These times serve as important places to review that what is being done with the patient is correct and adequate. Breakdowns can happen when during the review process the reasoning behind a choice is not explained, and the procedure looks incorrect.

In the observation notes below, a nurse asks the receptionist to set up a surgery for a patient at the hospital. Off the top of her head the receptionist recalls that that patient had the same surgery just a few months ago. When they do some further investigation, they realize that the receptionist was correct. What they decide to do, with the help of the office director, is schedule the surgery for a week and a half from the current date. That gives enough time to cancel the surgery if it turns out that it should not be done when the doctor gets back in town.

This kind of breakdown gives some indicators of problem areas. The first is that there is inadequate support for the documentation of medical procedures. While it may be difficult for doctors to list their reasoning each time, perhaps a list of typical reasons could be provided which could be easily selected. The second problem is that PC1 was only able to catch this kind of mistake because she was familiar with the patient. This kind of familiarity cannot be relied upon to catch mistakes. Instead, a system could support the review process that is already in progress to find mistakes.

In the second example, also from Med-P15, the echocardiogram administrator who visits that location occasionally to do "echos" on patients catches another time when the office ordered a stress test on a patient who had recently had a heart attack. While I was not able to watch how he noticed that mistake, I was able to notice that he went to the out-patient window to talk to PC2, and called to cancel the test immediately. The office then took care of the paper work in the patient's file. This kind of mistake could be easily caught with an electronic system checking the amount of time between critical events such as the last time the patient had a heart attack and a stress test.

Design implications:

- Support catching mistakes in patient's files by office staff who are reviewing a file.
- Support doctors documenting their choices for other office staff to review.
- Support testing for critical events in a patient timeline and have validation/explanation for why to override warnings.

Med-P15 Observation Notes:

*2010-08-20 1:55PM PC4 asks PC1 if she's set up a cath for a patient. PC1 says that she thought the patient has already been cathed. PC1 asks PC4 if she is opening up another cath line, what for. PC4 says that she is. They agree that the patient needs to talk to the doctor because the insurance isn't going to cover another cath. So for this patient they figure out that the patient was already "cathed" recently. They are confused why this patient is being called to be "cathed" again. They are concerned not just because insurance might not cover it, but because of the health of the patient. 2:42PM PC1 gets back on the phone to schedule a cath for the patient that they don't know why he needs a cath. She is talking to another internal person saying that she wants to schedule the patient, but that she needs to talk to the doctor before they are going to go forward with the procedure. PC1 gives the patient's name. She was on the phone with PC6. PC6 says that she'll schedule it for two Tuesday's from now. PC1 and PC4 talk about what their story will be about explaining why they didn't schedule it to the doctor.*

*2010-08-26 2:15PM The echo guy comes to the window with PC2. Turns out that this patient was scheduled for a stress test. The problem is that they didn't realize that he'd had a heart attack just a month ago. The echo guy gets on the phone to cancel the stress test. Seems like something slipped through that they didn't realize that he'd had this heart attack.*

### **9.33 Looking Up Patients on Sex Offender Website (Study 2)**

Observed

- Med-P15 2010-08-20 3:03PM

Patients have lives outside of the centers they are in. Unfortunately, this life can involve criminal actions – criminal actions that end up on national databases. Just because someone is a criminal does not mean that they also do not need care. The question becomes how much knowledge of this criminal action should be disclosed, if any, in a patient's medical record.

In the case outlined in the notes below from Med-P15, someone noticed in the local newspaper that one of their clients was being charged with having sex with a minor. Discovering that one of their patients might be in this sexual offenders database, the office spent part of their morning looking up other clients in the database. They found one other patient who was also in the database.

Is a case where the patient's privacy has been violated? I'm not entirely sure. I know that this is not information that is requested by the practice, and it feels like a privacy breach has occurred. This information can impact how a patient will be cared for. It is unclear that even if the practice were to discover that their patient's were felons that that information should be documented.

Design Implications:

- N/A

Med-P15 Observation Notes:

*2010-08-20 3:03PM PC4 jokes about wishing that the other computer was working because they could look up if their patients are sex offenders. Yesterday they were looking up people and found one, and it "floored" PC2. PC4 says that they don't know the whole story, so they can't judge, but they were pretty shocked. They were looking up local sex offenders and one of their patients... One of them, I think PC4, was reading the news that morning and saw a news story where they went into the house of a younger lady. This turned out to be one of their patients, who was an older gentleman. They then started to talk about him, and decided that they were going to look up some of their other patients to see if they were in the sex offender database. Well they found another patient who was in the sex offender database. Because PC2 was on the one working computer, PC4 couldn't use it as well. There is also a discussion about whether or not the person was really a sex offender, because they didn't know the whole story. I think this is some way for them to think through giving this person their care, while knowing that they might be a pretty bad person.*

### ***9.34 Pharmaceutical Representatives & Insurance Companies Seeking Patient Information (Study 1)***

Interview:

- Med-P10

In a second example, PL1 from Med-P10 was the only person interviewed who discussed a dislike of how much client information is provided to health insurances. He generally talked about his dislike of insurance companies, but one reason why he will not work with any of them is because he does not like how much information they ask to know. In his quotation below, he discusses how it is none of the insurance companies "business" whether or not the client is married.

In this example, the director and owner has decided not to use certain insurance companies because he does not want to participate in a system that requests copious amount of information (i.e., rules requiring patient information). However, because of the patients all use a certain kind of medical insurance, he is required to use some of them to stay in business. Therefore, even though he does not want to, he follows the rules. In

terms of analyzing the breakdown, the activity of maintaining his patient's privacy is in conflict with the activity of gaining payment for services.

Med-P10 Interview Transcript:

*Laura: So that's not just for Medicare but all insurance companies? It goes from the insurance company to the patient and skips you? (Right). But you still have to fill out the forms? (Right). So what kind of information goes on the forms?*

*PL1: Insurance ID number. Patient name, address, age, birth date, not all insurance ask for the birth date, Medicare does. Some of them want to know whether or not the patient is married, which is really none of their business but they want to know it. And Medicare can get away with anything.*

### **9.35 Pharmaceutical Representatives & Insurance Companies Seeking Patient Information (Study 2)**

Observed:

- Med-P15 2010-08-26 1:37 – 2:01PM
- Med-P14 2010-07-06 11:30AM

Pharmacology representatives visit physicians' offices regularly. As documented by Craig & Stitzel in their book "Modern pharmacology with clinical applications" in 2004 eleven billion dollars was spent on 'education' and 'marketing'. This involves providing "educational" lunches for the office where the pharmacology representative talks about their latest drugs. Most of the times this interaction was observed, though, it was pharmacology representative dropping off free food to the office staff and then talking with the doctors or office director to give free trials of a drug.

In one particular instance of a pharmacology representative visiting a physician's office for a "lunch and learn" the pharmacology representative was able to fax over all of the relevant information from a patient's file to her office. While it is unclear if this is against the practice's privacy policy, the patient was not observed to be contacted before the representative was given access to the file. The representative was able to go through the file and pick and choose whatever information was in it. This information was then sent off to another set of people who reviewed the information for their purposes. From observing the reactions of the people in the office, this action was not unusual.

In this case there is a breakdown between how patient's view who can access their information and who can actually view the information. The user is unaware of the additional people who are within their community. There is not a clear set of rules surrounding who can and does access patient's information, and what information companies should be allowed to ask for about a client.

Design Implications:

- Support listing an annotated list of who access and when a patient's information was accessed in the patient's record for the patient to review.

Med-P15 Observation Notes:

*2010-08-26 1:37PM ... Woman with blond hair comes and asks PCI for paper work... The blond haired woman gives PCI a name and PCI goes to get the file from the cupboard. PCI retrieves a file... PCI is pulling stuff out of the patient's file and handing it over to the woman. I think the woman is making a packet of information to fax over to another place. The woman is just tabbing through this woman's file. I did not get the impression at any time like this lady was a doctor, or even a nurse.  
1:46PM The blond woman returns to the side window with a big stack of papers and PCI starts to scan them. 1:55PM So PCI explained that after the talk at lunch they asked for a patient who might be eligible. They pulled the file of the patient, and the patient's information was handed over to the rep, and the rep pulled the information she wanted. That was what was faxed over to the reps company. 2:01PM The rep came by again, the faxing one, and verified that the file had been received. PCI asked what is going to happen next. The woman said that they are going to go over the file.*

Med-P14 Interview Transcript:

*2010-07-06 11:30AM Tracy talks about how an insurance company is asking for a marriage certificate of a particular patient. Her and Cassie are laughing about how ridiculous it is to ask for such a thing.*

### **9.36 Disregarding Privacy Policy (Study 1)**

Interview:

- Med-P04

In the interview snippet below from the director of Med-P04 he shares his feelings on HIPAA. While to a certain degree he understands the need for HIPAA, he believes that it is over restrictive of how he wants to manage his client's information. The example he provides is that he knows that he is not supposed to shout the patient's medical information in the waiting room. At the same time, though, he finds it overly restrictive.

This breakdown occurs because the local rules governing the activity of how PG1 desires to run his practice are in conflict with the Department of Health & Human Services activity of protecting a patient's information.

Design Implications:

- Support doctors and health care staff being able to report places where they feel that the policy is overly restrictive.

Med-P04 Interview Transcript:

*PG1: Anything that has a name falls under HIPPA. HIPPA as I understand it was developed to protect information that is sent over the internet. So like for example we have something called a VPN. Virtual*

*Private Network so it's like a pipeline between our offices and here, so nobody can get in. So that's a firewall in essence. So that's a HIPPA guideline. And then, the problem with HIPPA is, when it was going through congress a lot of people were throwing their pet projects on to HIPPA. So a lot of other goofy stuff got tagged on as well. Now HIPPA in my opinion, and I don't mind if this is recorded, I think it's a stupid thing. Now most of the stuff, with exception of the electronic transfer of information, the rest of it ought to fall under ethics not under law. Now I know there may be a fine line between there but I think it's an ethical dilemma. I wouldn't go out in the waiting room and say, you know, "hey Ms. Jones your syphilis test is negative," so to me it's an ethical thing and not a legal issue. Now maybe I'm not being fair. But they actually say, now my understanding of HIPPA interpretations, you're not even allowed to say the patient's name in the office. But what a load of crap, all that. I mean, when the patient comes in I'ma give her a hug, and love on her, and you know that's. If I got an 80-year-old lady, she wants a hug. I'm not gonna ignore her, you know, "205, you're up!" That's just, that's a little ridiculous. So that's my opinion.*

### **9.37 Disregarding Privacy Policy (Study 2)**

Observed

- Med-P15 2010-08-26 02:11PM
- Med-P16 2010-08-19 03:27PM

Interview:

- Med-P18

When patients first are seen at a physician's office they are provided a copy of the privacy policy that outlines what is a privacy breach and how the patient's information is managed. These policies are usually also framed on the wall in physicians' offices waiting rooms as shown in the pictures below. They outline the rights of the patient and how the records are managed, stored, destroyed, and who has access to them. Given the short period of time that new patients were given these forms and how long they were then turned over to the front office, patients were not observed to be taking extended periods of time to become familiar with the policy. We did not observe any attorneys being called to check on the patient's rights before signing the form. This disregard for the privacy policy makes the act of protecting the privacy and security denigrated. In specific examples, patients were observed at Med-P15 and at Med-P16 to say that they did not care about the privacy policy and that they were not going to read it. I assume that the patient signed the form saying that they had read it, even that was actually not true. In neither instance does the office staff tell the patient that not looking at the privacy policy is against their best interest. In fact, Nurse 2 at Med-P16 said that for all she cares about the privacy policy the patient can wall paper his bathroom with the paper. In both cases, these examples support a lack of patient knowledge about their privacy rights and at the same time demonstrates that the offices is also not serious about protecting the patient's privacy.

Med-P18 would not share her feelings about HIPAA when being recorded, but she did say for the recorder that many of her clients “don’t want” the privacy policy.

A privacy policy is merely a policy. It is an outline of proposed rules for governing patient information. It is no guarantee for how client information is actually managed. And, as can be seen from the theme ‘Discussion of HIPAA Violations’, and others, HIPAA has a much different meaning in the practice of managing client information than what is being stipulated. From an Activity Theory perspective, the activity of providing the client with a privacy policy lets the subject know the standard rules of how their information will be managed. However, the patient recognizes that there are other rules governing the practice of managing client information, and therefore disregards the privacy policy.

Design Implications:

- Support patients reviewing and asking questions about the privacy policy at a later time.
- Support the policies in the privacy policy, even if the patient disregards them.

Med-P15 Observation Notes:

*2010-08-26 2:11PM A patient comes to the window. He says that he doesn’t know how to fill in all the information on the sheet. She says she doesn’t need him to fill in that information, just the highlighted part. He has that part filled in. He asks what that other piece of paper is about. She explains that is their privacy policy, like most doctors’ offices. He says that he doesn’t want to see it. She says that he can keep that copy. He says he doesn’t want it. PCI tells him that he can just wait and someone will come and get him.*

Med-P16 Observation Notes:

*2010-08-19 3:27PM The patient comes to the window because he has filled out his paperwork. He hands back the HIPAA form. He made a joke about not needing this thing. Nurse-2 says that he can wall paper his bathroom with it if he likes. PBI starts to staple and highlight the papers that the patient returned.*

Med-P18 Interview Transcript:

*PO1: They can see it all, if they ask, they can see it. Umm we give them an notice of their privacy, privacy practices and we are required for each person that comes in, to offer it. Some people don't want it, but we have to offer it.*

### **9.38 Difficulties with Client Care when Outside of Office/Center (Study 1)**

Interview:

- Child-P01

Within childcares this issue is not related so much to the health of the child, but towards developmental and social problems that may be occurring. For instance, Child-P01 discusses how a child may be displaying a particularly behavior problem but when the child is at home the problem is not manifesting. Communication about what is and is not going on in the home can help the childcare manage turbulent transitions for a child. To help with these problems teachers from Child-P04 actually do an in home visit.

Design Implications:

- Support parents being able to document issues at home into a child's file.

Child-P01 Interview Transcript:

*Interviewee: "Sometimes the parents are dissatisfied with how a teacher arranged it. Occasionally, we try to put it very politely and nicely when there's a concern or we're noticing something's not happening, and they can occasionally get defensive in a conference. As, any parent would want to be, they want to see their child as a certain way and really when it comes to that front where, if we're like 'oh, they're four and we just don't see them counting past 10, that's kinda concerning for us, we're just surprised, he always stops at 10, doesn't seem to make it past 10 yet.' And, they can instantly kinda get the feel of where we're going--'well, at home, he counts to--!' That's what we need to hear, home and school's different and try to battle out there. But, more the complaints about the assessments and if they strongly disagree there's no amiable resolution. But, 9 times out of 10, it's 'oh, they're doing it at home, explain more situations, well that sounds great, that makes me feel better, obviously he must be doing something right, how are you getting it done at home, let's try it at school!'"*

### **9.39 Difficulties with Client Care when Outside of Office/Center (Study 2)**

Observed:

- Med-P16 2010-08-19 1:56PM

Interview:

- Med-P19

The care of patients extends outside of the office. This means managing the care of a patient when they have left the office and are at home. Unfortunately, both electronic and paper patient-management systems do not support the external care for a patient. This lack of ability to track patients when they are outside of the office results in a breakdown of patient care. Therefore, by gaining more knowledge of a patient and moving further into the patient's life can result in better care. This activity, though, is in direct conflict with maintaining the privacy of the patient.

In the observation notes below from Med-P16 with PB1, the office manager, is talking with an elderly patient. He has to take the bus to come to the office and whenever he needs to go to an appointment. He tells PB1 that while he can remember his appointment, it is a lot to remember for him to get his prescription filled before his appointment. It

involves him remembering a few days ahead of time to call the bus, go to the pharmacy, get the prescription filled, calling the bus, going home, and then remembering to take the medication the day before the appointment. He says that this is difficult for him manage. PB1 says that she will call him a couple of days before the appointment to remind him. She puts a mark in her calendar to remember to call him, but this message is not contextualized with the patient's information.

A second example from PS1 from Med-P19 demonstrates an alternative example that is a little less warm and fuzzy. PS1 talks about how she has to deal with patient's who have been using the office to gather prescription drugs and using different pharmacies. While it is in her office's best interest to make sure that they are not being used in that fashion, in this case she is trying to maintain the care of that patient to make sure that when outside the office they are using the prescribed drugs adequately and appropriately. Currently she has to go outside of the electronic record system to verify that the patient has not been abusing their prescriptions.

This kind of needed maintenance demonstrates the need for tools such as Bluetooth enabled medicine, sensor-based medication caps, and other in-home devices to extend client care out of the office. These kinds of tools would allow for a system to detect if the patient took their medicine before their appointment, or if the patient was taken too many medications at one time. However, the question becomes at what point does this kind of involvement start infringe on privacy rights of the patient. For those patients who remember to take their medications on time, and do not abuse the prescription drug system, do they need to have their behaviors monitored?

#### Design Implications:

- Support automated reminders for patients
- Build small out-patient events into the schedule
- Facilitate monitoring patients outside of the office
- Support parents being able to document behavioral problems at home as well.

#### Med-P16 Observation Notes:

*2010-08-19 1:56PM ...The patient is a chatty Cathy. When PB1 stops responding to him he starts to talk to me. She comes up with an appointment for him and he talks about filling out his prescription with PB1. PB1 puts the appointment into the computer. He says that he won't remember to take the medicine. Another patient has entered and come to the window. PB1 says that she'll make a note in the system, which she does, to call him a few days early to remember to get the prescription for amoxicillin. This medicine is an antibiotic, and because of the patient heart condition, he has to remember to get the prescription filled days ahead of time and then to take it the day before. He talks about how difficult it is because it isn't easy for him to travel everywhere.*

#### Med-P19 Interview Transcript:

*PS1: script to the pharmacy. You have, you got it all right there. Which pharmacy they use. The other way you can tell too is if they are starting when narcotics are involved, if you see them going around to skipping pharmacies you can see it. Yeah, that's a red flag. But that pharmacists are often, very nice to communicate with us if they know there is a problem too. So its kind of a two way street there.*

*Tom: How do you usually identify a trend like that, where they go to different pharmacies?!*

*PS1: There is a website umm, that is, here again, I think its the US, I'm not sure if its the government or not, but you, you can go on this website and it will tell you exactly what narcotics or what prescriptions they've gotten and who has prescribed them within the last however many days. And that's public information. They don't have to sign anything for us to do that or anything like that. So, if we suspect something, be it direct communication with a patient, we, there are certain red flags and if we suspect something, we just go on the website and nine out of ten times we're right.*

#### **9.40 Patient Information Left in the Open (Study 2)**

Observed:

- Med-P16 2010-08-19 3:00PM

Interview:

- Med-P18

Patient information is ubiquitous in these physician's office. It is on every desk, on post-it notes, and in files physically surrounding the office staff. With all this information about it is easy for patient information to be left out of a patient's file, or for a patient file to be left open where anyone can walk around and view the contents. This kind of openness is to be expected given the other breakdowns of 'Open Access to Client Information' and 'Not Knowing Who Accessed/Modified Client Information'. Everyone already has free access to information and what information they do access is not documented. Given these facts, it is easy to understand why offices would feel comfortable leaving patient files out and patient information open.

While I was not able to observe how the information was taken out of the file and left in the open, I was able to observe an x-ray that was left on the corner of PB1's desk from Med-P16's desk. It was only later that she went back and put the x-ray back in the appropriate patient file, with no explanation about why it was outside of the file. Additionally, PO1 from Med-P18 discussed in her interview how they have everyone, including the cleaning staff, sign privacy policies to protect the fact that information will be left out.

Leaving information open represents the activity of making work visible for returning to it at later time. However, it is in direct conflict with keeping the information secure in the sense that it is not locked away and protected from prying eyes.

Design Implications:

- For information taken out of a patient file, support tracking it to know where it went to and who was likely to have seen it.

Med-P16 Observation Notes:

*2010-08-19 3:00PM ...when Nurse-2 was in here 5 minutes ago she pulled out an x-ray that is in a stacked binder to the right of the monitor, looked at it, and then put it back. Just a random x-ray sitting on the desk - not in any file.*

Med-P18 Interview Transcript:

*PO1: But it's basically letting them know that the fine umm because obviously they are going to come in and see things laying on the desk that pertain to patient information. Once their, the company they work for is bound in that contract, we're protected.*

### ***9.41 Inability to use Electronic System Results in Information Duplication (Study 2)***

Observed

- Med-P16 2010-09-09 2:55PM

The example below offers some insight into the power of paper systems over electronic systems and why there is a disconnect between them. In the example below PB1 from Med-P16 is working on her “ticker file”, which is a file of all the patients who have missed their last appointment and need to be “tickled” into returning. This file is completely electronic and managed through the electronic record system. However, the doctor has PB1 print out the file where she goes through it, does all the work, and then re-enters the information back into the electronic file. She says that she does it this way because the doctor likes to look over her work. In this case the creation of extra information and an extra place for patient information to be leaked is due to the fact that paper affords oversight. Because paper has this affordance, it is the tool used in the activity of managing office procedures, rather than the electronic system.

Design Implications:

- Mitigate reasons why paper is still used – such as poor oversight tools in the electronic system.

Med-P16 Observation Notes:

*2010-09-09 2:25PM PB1 shows me what she is working on. It is called a 'tickler file'. It is a list of patients who she needs to follow-up with. If a patient has called to cancel an appointment or they are being referred over and they couldn't get a hold of them, the note for why they person wasn't scheduled is put into the electronic system. Then she prints out a file of all the people who she needs to call and sometimes she writes notes on the papers. She has to print it out for the doctor - so that he can check up on them - because he doesn't know how to use the electronic system.*

### ***9.42 Restricting Client Access to Files (Study 1)***

Interview:

- Med-P01
- Med-P02
- Med-P04
- Med-P07
- Med-P08
- Med-P11
- Child-P01
- Child-P02
- Child-P03
- Child-P04

For instance, in the interview notes, PD1 from Med-P01 explains that a patient is not allowed to access their records. When asked why, she explains that the patient would not be able to understand the notes about the patient. She later explains that even when a patient moves offices, they will instead fax the patient records over rather than trust the to the patient. An example of this was observed also and included in the observation notes below. The patient was given a business card with the locations information on it. The patient then was told to give that card to their new office and the two offices will negotiate transferring the files.

Other reasons stated by other directors of physicians' offices for not allowing the client full access to their files are that they would not understand the record, because the technology does not currently support really sharing the information between the office and client, because the client does not actually own the information, because they do not want to loose their original record, because there might be information that they do not want the patient to know they are recording about them (e.g., being obnoxious), because they do not need to see all of the information but only a summary of what has been done, and because the patient should only have access to a copy.

Different from physicians' offices there was more of a spectrum over what parents could and could not see in their child's file. All childcares except one, Child-P02, said that parents could come in and view the child's file within their office – usually with supervision. While this appears as more open access, the director explained that she would usually stay in the room with the parent when they were looking at the file. This surveillance creates a kind of restriction for the parents being able to thoroughly examine their child's file. This serves a purpose. Childcare directors explained that they would sometimes keep sensitive information towards the back of the file. The director of Child-P02 said that the reason she would not want parents to look at their child's file was because she had made notes about the child or parents that she would not want them to be able to see.

While parents were not restricted from examining their child's file, there was other information in the childcare that parents were not provided the ability to access. These

include the logs that teachers keep in their rooms of daily activities, videos that were kept and stored of a child's activities, and logs of suspected child abuse.

This kind of breakdown reflects a lack of rules surrounding the ownership of the information. The rules surrounding who owns the information are different from office to office, making a grand rule impossible for clients to know and understand their rights to their information. This lack of a rule puts the onus of information management onto the office, thus relinquishing most of the client's responsibilities to manage the information. This power and authority then allows the office to dictate how the information is transferred and annotated. Overall, this breakdown reflects a lack of rules surrounding the division of labor of managing client information between the subject and community.

HIPAA requires that patients be allowed to access their files. While childcares do not have a mandated law, it follows that clients should be allowed to access their own information to at least check that there are no errors. However, what we found is that there were differing ideas that would restrict a clients ability to access their information.

Design Implications:

- Support showing what information the client provided
- Support layering client information with annotations that the client may or may not be allowed to see
- Support sharing client information that they would be able to review

Med-P01 Interview Transcript:

*Laurian: Can a patient access his or her own record?*

*PDI: No*

*Laurian: why not?*

*PDI: Because they don't understand what's in their record. They wouldn't understand because we have short notes on the back of their chart, and they wouldn't be able to read it.*

...

*Laurian: So the patient can't access their files; so what if a patient moves, what happens to their files?*

*PDI: We will send their files to the orthodontist they're going to see.*

*Laurian: Okay so the only reason that a patient can't access their file is because they won't understand it. Is there anything in their charts that you wouldn't want a patient to see?*

*PDI: No, they just wouldn't understand it. Plus if they're transferring to another orthodontist, we know they won't lose their records because we send em via UPS.*

Med-P02 Interview Transcript:

*Laura: Can a patient access their own file?*

*PQI: No.*

*Laurian: Is there a reason for that?*

*PQ1: Well if they ask I guess. But we have a Dentrex program, so I don't think they'd understand that. It's a dental program.*

Med-P04 Interview Transcript:

*Laura: ...So alright. We talked about information that they provide when they first come in. Can they [patients] access their own files?*

*PG1: No.*

*Laura: Why is that?*

*PG1: Technology, we just don't have it, availability. Now if they requested a copy we'd give it to them, but. (Okay, so like their treatment plan or something?) Yeah. But this is something just for information for you, the information in a file belongs to a patient, but the file itself belongs to the doctor. Does that make sense? So and the same thing goes. So people think when they get an Xray they've bought an X-ray but no, the information on the X-ray belongs to the patient but the actual film itself belongs to the doctor. So I know it's a little screwy, and we don't argue with patients about it, you know. That's right. You know, but unfortunately due to technology we don't have access. And I tell ya, I think it'd be a hard day before someone can sign on and then access their file.*

Med-P07 Interview Transcript:

*Laurian: Does the patient have access to their own files?*

*PA3: Yes. If they request it we have to give it to them.*

*Laurian: So do you hand over the physical file?*

*PA3: No, we make a copy and give them a copy. We never release the physical file.*

*Laura: Do people ever ask for that?*

*PA3: For a copy? Yeah, mainly if they're moving. And we do a lot of, we write their glasses prescription on a prescription pad for them because a lot of people want to keep it in case they travel and need to get glasses again.*

Med-P08 Interview Transcript:

*Laurian: Okay and just to follow up on the question about anything you wouldn't write down, is there anything you wouldn't put in a patient's file but that you might know about a particular patient?*

*Laura: Like one example that I can think of would be if somebody came in and they were just belligerent...*

*PII: Oh, yeah, sometimes we'll just let the doctor know if somebody's having problems like that we'll stick a post-it note on the front of the chart just to give him a heads up, and then we'll shred it, like we've had a couple people fuss about the handicap ramp, it's not so good, but he's working on that. But we'll let him know, you know, say something to the doctor, put a note on there just to give him a head's up that they may say something. That kind of thing.*

Med-P11 Interview Transcript:

*Laura: Do parents ever ask to see a copy of the whole file for their child?*

*PC6: No we don't give them the whole file. There's a limit to a one page thing, but it's basically treatment that we've done, if there's any treatment that they need to have done, if there's any sedation type information that we did us, and what we did at that time, and then what the recommendations are for future treatment.*

Child-P01 Interview Transcript:

*Interviewee: They're allowed to access anything in their child's file they just have to come to a director to pull that file... we're not going to just let them have free access to our file cabinets but a lot of the times if it's 'oh I need to see their health record because they're going into a summer camp that requires it, can i make a copy'... everything in that file is theirs, they own that. They own the child, they own those papers. They wrote on them, they signed them, it's theirs. Basically we're just borrowing them if you will, and borrowing that information so they just need to ask for permission to get to it then we literally pull it out for them and we're standing right there with them.*

...

*Stacy: "Is there anything in the child's file that you wouldn't want the parents to see?"*

*Interviewee: "Noooo, but. It's again, when it comes down to reporting a case of abuse or neglect, I mean, it's hard when we're collecting information. We have to act pretty quickly, but at the same time we don't want them to see, like especially if it becomes an unfounded case--be like 'why are you collecting this information, you're saying I'm a bad parent'--so, we try to keep that stuff kinda separate and aside and away so that it's not necessarily 100% visible. If it doesn't come to fruition, if licensing does step in or social services steps in, you know, then it becomes a more prominent feature, because obviously they know about it. But, it's a tricky line, you know, the owner and I were talking about it not so long ago. It's scary for us because you never know how a parent's gonna react and technically we're supposed to go to Social Services before we go to a parent, but you know what if there's a case where you know, you know family strife is going on, and it's very stressful right now, and what is the real story--is it a matter of frustration at the moment. You know was it a one time thing and so what's the right thing to do--really go to Social Services and risk the child being yanked from the classrooms, their home life, and an already stressful environment that will move on and be happier. Or, you know, go to the families first and say 'hey, we're noticing things and we're concerned for your family. But, really we do try to keep that kinda separate until things are discussed."*

...

*Interviewee: "If we're collecting information on a possible abuse, or a possible developmental thing, that's kinda kept up and away so that we*

*can finish collecting it. We don't want parents to get upset and overwrought and then skew things out of proportion"*

Child-P02 Interview Transcript:

*Laurian: this is great, thank you... ok so that will give us a lot of information about what they provide.. what is the kind of information that they can access?*

*P2-A: we have a website they can look at .. we don't usually let them see the children's files because it has notes possibly even about them and things like that==*

*Laurian: ==mmhmm==*

*P2-A: ==about the child so we don't want them to see anything like that... we're working on sending home newsletters*

Child-P03 Interview Transcript:

*P01: Because I don't need the original once they are gone... you know, that's just...not if I have to do, I just do. But some parents would say, 'Can I have my proof of birth' too, cause they are too lazy to go home and do that again. And I say no, because what I have on record your center cant see. They have to see the original to verify themselves that that's your child. I have done that work and your new center is supposed to do that. So you cant have mine, no. And I will tell them they cant.*

*Tom: do you record that?*

*P3: it is recordable but it's main for our benefit, it rotates classrooms every 30 seconds so that we can just keep a visual, there's no sound. It rotates to 16 camera locations, I think, throughout the building and the outside but we're having some issues with our system period, the alarms are going off every morning until about nine, nine thirty so we're trying to figure out what's going on but today when I turned my camera on that's what it was doing so I'll check my cables and cords later when I got time to*

*Laurian: is this the only place where that==*

*P3: ==we can pull it up online as well they - at the front desk they can pull it up to monitor from a location I'm not really sure where... I've never had to do that because my desk was always in here but they are able to pull it up at the front desk*

*Laurian: so how do people get access to that?*

*P3: they don't. It's not for the parents... we did some off the cuff research ourselves when building this building on the the cameras and centers that use them for parents to get online and watch and then centers that had them and didn't do that and parents, of course, love it, that's a given to have that ability to look into their children but some of the centers that I contacted that would give us information said the big downfalls are if you got those parents who - "why is Johnny crying? I just saw so and so push him" and I don't have enough time in the day to do that all day long and - you know, if a parent calls in with a concern you have to take care of it so*

*you have to call the classroom and, you know, you want a parent to feel that you've checked in on the situation and I don't have all day to do that and we have a large facility so that would be - and I know the systems you have online, they time out.. you can only stay on for a certain amount of time but you can log back in from what I understand and I had some director say that "I've got parents staying on all day and I get phone calls all day" and so we decided - we put it in for our benefit anyway so we could monitor evals on lunch like you can watch to see if hands are getting washed, what's going on at the lunch table without being in the room and the teachers literally forget that it's there so it's really good... so if I wanted to station it on just a particular classroom and watch some new staff that we've hired or some new children to see how they're progressing in the classroom I can just lock it on a certain classroom and leave it there or it will rotate through every 30 seconds if I'm busy and not really watching it but if I'm not sitting here then PP2 might be sitting there and watching it or PP3 might have it up at the front desk so it's mainly for our benefit anyway.. we had some parents that were kind of like "aww, really?" because it - just for us right now that's just the purpose we wanted it for anyway, for our benefit*

Child-P04 Interview Transcript:

*Tom: and do you keep any information on them that they don't provide themselves?*

*P4: we do use documentation when something occurs with a family that we don't make accessible to that family... that's between staff members... that's confidential information that we will document and keep... if I were to have a conversation with a family I would document that conversation - typically if it wasn't just a normal conversation, if it was anything that had a risk factor to it then I would document it, and that's not accessible to them, that's my personal information*

### **9.43 Restricting Client Access to Files (Study 2)**

Observation Notes:

- Med-P01 2010-06-07 9:40AM

Interview:

- Med-P18

Some physicians' offices restricted patients from accessing their own records. In data from Study 1, the directors had a multitude of reasons for doing this. In the two cases from the observations and additional interviews, this finding was reaffirmed. The observation notes show the only time a patient tried to ask about their records in all of the observations. The practice deflected the patient's father explaining that they would forward on the patient's records to the next orthodontist. In the interview transcript the participant explains that if the patient wanted to see their file the patient would instead be printed a copy of the file. While printing does not necessarily mean that the office is

deleting or filtering the file, it does allow for an additional filtering step. There is also no way for the patient to verify that they have all of the information.

In these breakdowns, the lack of known rules surrounding a patient's ownership of their files creates ambiguity in the activity thus resulting in a breakdown.

Design Implications:

- Provide methods for patients to see the information in their file.

Med-P1 Observation Notes:

*2010-06-07 9:40AM PD4 appears in the doorway with a boy (~10 years old) and a man in his 30's or 40's (boy's father?) at 9:40 am. PD4 shows the man something by gesturing to the boy's mouth with her hand and then tells him to let them know once they find a new orthodontist and they will send his notes over.*

Med-P18 Interview Transcript:

*Tom: So they can access their own file whenever they'd like?*

*POI: We can print it for them.*

*Tom: Okay.*

*POI: Of course they can't go in our database.*

#### **9.44 Not Knowing Who Accessed/Modified Client Information (Study 1)**

Interview:

- Med-P01
- Med-P02
- Med-P03
- Med-P04
- Med-P08

When a client's file has been accessed, it is hard to know who accessed it, what has changed, and if the action was necessary based off of the audit trail present in either a client's paper or electronic file. Similar to the breakdown 'File Being Kept Outside the Office', there is a lack of transparency. Part of this problem is that some electronic systems do not actually support having multiple passwords. A larger part of the problem is that the users do not use the passwords. The largest problem is that interfaces are not user friendly for accomplishing work quickly.

In the interview notes from Med-P01, PD1 talks about the fact that anyone in the office can access and modify the client's information. This is part of the job of working in this office: accessing and modifying patient information. The problem arises when there are errors: patient records being incorrectly filed, a missing patient file, and incorrect information in the file. Figuring out how these mistakes happened in order to stop them from happening again is hard to reconstruct, resulting in continuous breakdowns. However, this need does not overwhelm the desire for open access; it is not a large enough concern to change the current method.

The problem is that with physical files afford more secondary surveillance. For instance, if Jane is seen over with the files in the 'B' section, and the file for "Baggins" is missing, or has been misfiled, the office staff knows to discuss with Jane to see if she knows where the file is. With electronic files, all access looks the same. Visibility of the work stops the group from being able to socially manage the information security.

Logging in to the computer is so incongruous to the work that people are doing, that P11 and Med-P08 discusses a secondary way that they use to determine who has made a change in a client's file. Even though everyone has the same access, but has individual passwords, people still put in their name when they make a change to notes on the patient. This allows them to see who had made a change if it is incorrect. Apart from this, only one other office in the nineteen offices mentioned that logging of who had made changes was used, and this office was connected to a hospital with a much stricter access policy. Tracking who did what is so secondary that it is not consider useful.

The breakdown occurs here because this task is so secondary; it is impossible to track down when a privacy or security breakdown has occurred. This is not to say that the office does not care about security or privacy, but more that they are currently incapable of supporting novel ways of managing security and privacy through the adoption of electronic records.

Design Implications:

- Support other ways to track who has accessed what patient information

Med-P01 Interview Transcript:

*Laurian: Who can access the computer system?*

*PDI: Anybody. Any of the employees.*

*Laurian: Is there a record of who has accessed what files?*

*PDI: No.*

*Laurian: So who can add or modify any information in there?*

*PDI: Any of the employees*

*Laurian: Is there a login?*

*PDI: Yes*

*Laurian: Is it for everyone in the office, or individually?*

*PDI: It's just the one login – just in general*

Med-P02 Interview Transcript:

*Laurian: Is there any kind of audit trail about who has accessed what files?*

*PQ1: Not that I know of. But this is kind of all new to me so I'm not sure if...*

Med-P03 Interview Transcript:

*Laura: So everyone that works here can access the computerized system? (uh huh) Is there an audit trail, like can you keep track of who accessed what files, or look into that if you wanted to?*

*PF1: Uh, I don't think so.*

*Laura: Can anybody add, modify or delete information from the system? (yep)*

Med-P04 Interview Transcript:

*Laura: And anyone that works there can access the system with their login, is there an audit trail of who's looked at what on the system?*

*PG1: Uh that's something we're going to need to look at but no we don't have anything of that nature. We don't even have the system up yet.*

Med-P08 Interview Transcript:

*PII: Yeah because it doesn't show who's logged in and most of the time I'm logged in in the front because I'm the only one up there, but occasionally someone else will come up and they'll just do it, and I usually check to make sure just because it is on my login, but that's one thing is we wanted it to actually show who's logged in. Because you can make the appointment, click out of it and go back into it and see who's initials are in it, and then in that case you can click on the box and then we'll put our name so they'll know who really made it.*

### **9.45 File Being Kept Outside of the Office (Study 1)**

Observed:

- Child-P03 2009-10-13 9:36AM

Interview:

- Med-P02
- Med-P04
- Med-P08
- Child-P06
- Child-P12

When patient's come to a physician's office they are likely not thinking about the lifetime of the information they are about to provide. The minimum amount of time we found that a physician's office kept a client's records was seven years. There are numerous physicians' offices that never delete a record, with one office inheriting files from the 1930s. While not getting into the why people keep records for so long, there simply is not enough space at the physician's office to store all of those records. For that reason, many records that are past a certain span of years are moved to a secondary location that is outside of the office.

Moving files to an offsite location has two sides. The first is that the files are stored in locations such as basements, central storage facilities, and "storage". Basements more than the other two have concerns about safety and security of the files. All, though, bring in a new set of people who now have access to a client's files that were previously not

accounted for when the client was probably constructing a mental list of who would be able to access their files. To be clear, this is a discussion only of a patient's physical file. Many interviews also discussed how physicians and health care workers would make back-ups of the electronic system and store them at their home. The point is that the network of access is actually much larger than first conceived of, and visibility of access logs is almost non-existent. Clients have no knowledge of what is being stored in these facilities, the security measures to protect them, and what will happen to the information if it is stolen.

The directors of Child-P03 and Child-P01 were the only childcares who reported destroying all or part of their files after a child was no longer in their program. For example, after children left copies of their birth certificate were destroyed. The remaining childcares reported that their files would be stored indefinitely. Some of these used external locations to store their extra files. The reason for indefinitely keeping a child's files was best summarized by PP1 from Child-P03. She explained that it again comes down to children being a protected class of citizens. While she would hate to think that any child was ever abused within her childcare, she needs to have the documentation ready to support whatever issues may occur in the future after a child turns eighteen and they have the legal right to pursue a legal case. One childcare said that he kept all of his child's files because it was required for licensing.

The breakdown occurs because the activity of keeping client information overwhelms the activity of keeping client information secure.

Both childcares and physicians' offices were also observed to have taken files home with them where additional people could access the information. For example, Med-P16 had a doctor with a "homework pile" that he took home with him each night to do things like calling patients to make sure they were recovering well. PP2 from Child-P03 also reported that she had files in her car that she forgot to bring in.

#### Design Implications:

- Support greater transparency over the physical location of where a client's information is stored.
- Support a viewable access log of who has viewed a client's information.

#### Child-P03 Observation Notes:

*2009-10-13 9:36AM During this conversion PP2 mentioned that the accident file is in her car. She took it home to work on it and left it in her car this morning. She forgot to bring it in the center. It's interesting to see that they staffs take files to their home*

#### Med-P02 Interview Transcript:

*Laurian: Okay. How long do you keep your records here?*

*PQ1: We keep them 7 years; we have a file cabinet upstairs for the ones that haven't been here in the last 5 years but we keep them for 7 years.*

*Laurian: Okay what happens afterwards?*

*PQ1: Well actually Dr. Glasgow still has them. He has them from when he started 20 years ago.*

*Laurian: Are they stored somewhere else then?*

*PQ1: Yeah he keeps them in his basement. As long as I've been here- the old office, we didn't have room for storage.*

...

*PQ1: Well they would tell me why first. I would need to know is that patient coming in? There's no reason, and every night the files are locked. That file system that he just got us, we lock it. And if it was broken into nobody could get any of those out.*

#### Med-P04 Interview Transcript:

*PG1: Well no, we have a central storage room which is actually in the back of our Fairlawn office. So at the end of every year we give a list to all of our offices of everybody that has been in in the last 3 years. So we keep those files and all the other ones get moved down to the central storage facility.*

*Laura: So you really are drowning in paper, then!*

*PG1: Oh yeah, we've got thousands of files. I bet you that we have 10,000 files. Well that was before [NAME]'s clinics. I bet we have 15,000.*

#### Med-P08 Interview Transcript:

*P11: Yeah when he took over for the other doctor he got all of his records. He's probably got back to 64, 74.*

*Laurian: where are those old records? Are they still here?*

*P11: Oh they got 'em in storage till they figure out what they're going to do with them.*

#### Child-P06 Interview Transcript:

*P6: staff files we keep physically for current employees, now children and staff - once they are no longer employed here or no longer enrolled here we do take them - we box them up and they are taken to secured storage*

*Tom: so there's an offsite place for information?*

*P6: yeah, for previous families - i mean they're all accessible but, because the center has been open long enough, we just don't have the physical space to keep that many*

*Tom: so how would access to that work?*

*P6: i've not been to the storage facility yet... right now the people who are the owners of the program are mainly the ones - when a box gets filled up i call them and tell them and they come and take it for the storage facility for us so they would have access, i would have access - we have an assistant director and if she had a request then she probably could but beyond that there's probably not going to be other people*

#### Child-P12 Interview Transcript:

*P12: yeah, for three years... stored here for three years and then we put them offsite*

*Tom: how does the offsite thing work?*

*P12: Owner1 and Owner2 each have - he owns (???) Mills so they have some storage space they have available that they have there in that building and they have some that's specific for files and stuff so we can store them there but we won't have to worry about that until three years*

*Tom: so after you start storing stuff who would have keys?*

*P12: the owners*

### **9.46 Open Access to Client Information (Study 1)**

Observed:

- Child-P03 2009-10-13 8:44AM
- Child-P03 2009-10-13 9:45AM
- Child-P04 2009-10-26 9:41AM
- Child-P06 2009-10-22 1:55PM

Interview:

- Med-P01
- Med-P02
- Med-P03
- Med-P07
- Med-P08
- Med-P09
- Med-P10
- Med-P12
- Child-P01
- Child-P06

In all of the observed physicians' offices the client files were openly displayed for anyone in the office to be able to access. An example is shown in Med-P01 where the files span the office space of the medical director and staff. While there are certain place-based and role-based norms that are regulating who can access this information, as discussed in the dissertation proposal document, regarding how these files are left open clearly represents a security breakdown. These files hold highly sensitive information, and the fact that they are freely available for anyone to be able to access illustrates that they appear to be not very secure.

To try and understand why the files would be left so open, quotations from eight of the director's of the physicians' offices are included below. These quotations illustrate how anyone in the office can have open access to all of the client files without restrictions. Perhaps the most representative of these quotations comes from P11 at Med-P08 who said in response to if someone has access information that they shouldn't, "I don't think so, because most of the stuff that we have here is just stuff that we can always access, so there's not really anything we can't get into." Or, even more direct, for small physician's offices, the director from Med-P10 said when asked who could access all the information, "Both of us do, yes." When there are only two people in the practice, you know that if

something was changed who was the one who made the change. Having restricted access can become a little ludicrous when people have to wear so many different hats to accomplish all of the work of the practice.

Childcares also had similar issues regarding keeping client information in unlocked locations. Many of the childcares reported that they the child's files were stored in locked offices or within locked filing cabinets. However, this was never actually observed. Within three of the childcares that reported that they locked their files, when they were observed a key was never used and the observer checked when the director was out of the office that the drawers were open. While the files in childcares are usually stored within drawers of filing cabinets rather than on shelves like physician's offices, access is almost as readily available.

Open access to client information has many functions. The files are easier to access when the office becomes busy. It keeps what work needs to be done more visible by showing places where files are missing. It signals to new clients that they already have repeated successful business. However, it also means that the information is more available to steal. The problem is that these businesses do not have a clear embodiment of who would steal the information. When they are surrounded by the information day in and day out it means that they can become innocuous to the importance of that information. Therefore their activities that keep the information more readily available override any activity of securing that information.

#### Design Implications:

- Support automatic locking of files when someone is not present with the files
- Support heat mapping where people are for odd times when people are accessing files, or accessing files when only one person present.

#### Child-P03 Observation Notes:

*2009-10-13 8:44AM The notebooks I saw open earlier that PP3 was working on are still open. This teacher is looking at the notebooks and other files. She is not brushing through the data, she has her full concentration. She is an older woman, in her 50s, with an apron which makes me think that she might also work as a kitchen staff. She is reading the files without any kind of hesitation. It looks like she doesn't care if someone sees her reading those files.*

*2009-10-13 9:45AM PP2 goes to the director's desk and pulls out a file from the bottom drawer which doesn't seem to be locked. She tells me it's a file of a new employee. She needs to see some information. When I was there they opened a lot of drawers but I have never seen anyone using a key to open any drawer.*

#### Child-P04 Observation Notes:

*2009-10-26 9:41AM I realize that I have left my phone in PUI's office and go back to get it for timestamps. When in the office, the door to which is*

*still open and lights are still turned off, I check the top drawer to the cabinet where active children's files are kept. ["I feel evil" was my comment to myself at the time; I felt very uneasy breeching trust like this and decide that I won't do anything like it again]. The drawer opens. I see several manila files for children inside, but close the door immediately, having only opened it a few inches. I return to the kitchen and write down my note.*

Child-P06 Observation Notes:

*2009-10-22 1:55PM There is only a file cabinet with 4 to 5 drawers. It does not appear to have any locking mechanism. No keyhole in any corner or in the drawers. None of the drawers are labeled except of the one on the bottom.*

Med-P01 Interview Transcript:

*Laurian: Who can access the computer system?*

*PD1: Anybody. Any of the employees.*

Med-P2 Interview Transcript:

*Laurian: So who can access a patient's file?*

*PQ1: Whoever's taking the patient back gets their chart, and the doctor*

*Laurian: Can somebody who's not working on the patient access their file?*

*PQ1: If they go into the computer, they can.*

Med-P03 Interview Transcript:

*Laura: How many people here have access to all the files? Does everyone that works here have access to patient's files?*

*PF1: Yes. Mmhmm.*

*Laura: How is access to information on the computer managed? Is there a login? A password?*

*PF1: There is no login for the software; there's a login for the computer, but during the week we keep the computer pulled up.*

Med\_P07 Interview Transcript:

*Laura: Okay and does everyone in the office have access to the patient's charts and the billing stuff too? (yes) Has that ever changed? Did there ever used to be restrictions to access? (no) Okay, great.*

Med-P08 Interview Transcript:

*Laura: Has there ever been a time when somebody accessed information they weren't supposed to?*

*PII: I don't think so, because most of the stuff that we have here is just stuff that we can always access, so there's not really anything we can't get into.*

Med-P09 Interview Transcript:

*Laura: Alright, does everybody who works here have access to all the information about patients? Their charts?*

*PT2: Yes*

Med-P10 Interview Transcript:

*Laura: Does everyone who works here have access to all the patient's files?*

*PL1: Both of us do, yes.*

Med-P12 Interview Transcript:

*Dr D: Yeah I've heard that, I mean, there are 4000 employees of Centra health. But I have heard that people have gotten fired- I mean, they tell the nurses and doctors, but the doctors are for the most part not employees of the hospital. But they tell the hospital employees that if you're caught looking at the wrong chart, you're fired. And I've heard of a couple of times in the last 5 years where that's actually happened. The nurses I have to say are very skittish about that. Making sure they don't access or look at something they're not supposed to look at. And they don't. It's really, because of the seriousness of it, it's really taken very seriously. Now this, this is different. To look at the schedule, anybody who knows the username and password can, it's just one. But in order to get in and look at patient records you have to have a username and password that's individual, that's linked to me and to any other individual here.*

Child-P01 Interview Transcript:

*Interviewee: "The physical environment has changed--I mean I know that it has a very similar layout. But we bought a lot of new furniture, a lot of used furniture. And, I know one of the questions you asked me in the past was, you know 'are the files locked?' Well, no... Not in the sense that the cabinet gets lost, you can see that I'm missing a key lock. But, traditionally, there's always someone in the front office here, either in my office or the office next door. So, if I need to step out, I can leave my door open knowing that my office mate is going to be looking for, you know, anybody in my office. Otherwise, the door is shut and locked behind me."*

...

*Interviewee: "Since there's a director always there, teachers are bound by confidentiality, it's in their agreement, it's in our handbook, any violation of confidentiality is immediate grounds of termination. We try to use a lot of trust. Pretty much, there's nothing--more often than not there's not anything that they can't see. Um, there are cases of children that you know we've had suspicions of abuse or different information, but we kinda want at the same time for them to be privy to that so that you know if there is a future concern, if it's a child that we feel's being neglected and he's coming in and he's unclean every morning, we have to bathe him, or he's coming in with fleas on him. You know, we want them to kind of know*

*ahead of time. If it's been a resolved issue, then we kinda let it go, but if it's something that's still on the fencepost of what's going on, you know, we talk to their Social Service agent before or whatever the need might be, we want them to be on the lookout."*

*2010-10-14 10:30AM "I know that they have a strict policy on who they let see which information, do you have a policy that is influencing theirs about 'the teachers can only see...'"*

*<shakes her head no>*

*"no, ok"*

*"each... for the children's records, no, for the staff records, we don't necessarily have anything. But, they're supposed to keep them confidential, which means that staff wouldn't need to see other staff. But, for children, the staff can see the children."*

*"so, technically, all the teachers could see all the things from the records"*

*"yes, they just go above and beyond. Which is fine. As long as our minimum standards are being met, they can go above and beyond."*

#### Child P06 Interview Transcript:

*We do... the children's files are all kept here in this filing cabinet... They are - teachers do have access because there is information in them that the teacher may need to see... emergency contact information - now we do try to keep copies of that in the classrooms but every once in a while we need additional information that's not listed in the classroom so they, within reason, ... - there's not a real clear [procedure] where you have to come in and sign in in order to come in and do it but they are kept in my office to limit so that there usually is someone who is observing - I mean the staff don't just come and peruse the files*

### **9.47 Open Access to Client Information (Study 2)**

Observed:

- Child-P01 2010-09-08 1:29PM

Most of the data for this theme came from the Study 1 data, but there was one instance in observing Child-P01 where a teacher came in and freely accessed a child's record. What is important about this fact is that Child-P01 is an accredited childcare that askses parents to restrict who they would like to access their child's file. There is no way for the director to know whether or not the parent had restricted that file without her first looking, which did not happen in this case.

The breakdown in this instance occurred because there was an explicit rule stated by parents and the childcare surrounding information access. However, the practice is different from the rule.

Design Implications:

- Support automatic logging of how accesses a client's file and allow clients to audit this log.

Child-P01 Observation Notes:

*2010-09-08 1:29 While the form is faxing a woman comes in and asks if she can get something out of a child's files. PT2 says sure. The woman goes into the filing cabinet and retrieves a blue piece of paper. She leaves.*

### **9.48 Lack of Knowledge of What to do If Something Goes “Wrong” (Study 1)**

Interview:

- Med-P02

Similar to the breakdown of ‘Lost Paper Patient File’, this breakdown is about the lack of knowledge of what would happen of an electronic file was missing. There is a mental model of computing that says that a file cannot go missing unless someone explicitly deletes it. When asking directors of physicians’ offices if the system had crashed at some point, most responses were no, but there was one who responded that they would not have known if it did crash. This lack of knowledge about the electronic system means that the care providers are incapable of being responsible stewards of the sensitive personal information. There is little visibility of what changes to the system have occurred, and this lack of visibility results in the care providers being unable to detect tampering with their system.

Once knowledge of what could go wrong becomes visible, care providers could then learn about how to deal with what happens after the system no longer works.

Design Implications:

- Support simple visualization of changes to the electronic system. For instance, if in one day there is twice the “normal” number of changes to electronic records, this should be displayed in red for the health care worker to investigate. Or, if a file was accessed where a person was not on the schedule, this should also be flagged.

Med-P02 Interview Transcript:

*Laurian: And what would happen on the electronic system if anything suspicious were to happen. Like if a patient's file went missing?*

*PQ1: Oh gosh I don't know. That's never happened so I don't know.*

### **9.49 Electronic Record Systems Crashing & Loosing Client Information (and Fears) (Study 1)**

Interview:

- Med-P02
- Med-P03
- Child-P03

Eighteen out of nineteen physicians' offices had some form of electronic records to manage their patient's care. All twelve of the childcares also had electronic system. All were asked if their system had crashed at some point. Most responded that if it had, they did not notice, or 'no'. Two directors of physicians' offices did answer that their system had crashed and that they had lost client information. Med-P02 discussed how they lost all of their account information for their clients. They had been making electronic back-ups at the time of that information, but it turns out that system had not been working for three weeks when the fatal crash happened. This resulted in PQ1 spending many weekends re-entering the information into the electronic system from the paper records that they were still keeping. Similarly PF1 from Med-P03 discussed a virus that destroyed their client's medical and account information in their system. This crash has resulted in the office keeping paper copies of all of their records and doing additional electronic back-ups of their system.

#### Design Implications:

- Present a visualization of the back-up process to care workers so that they can see whether back-ups have been successful.
- Periodically force care workers to access files from the back-up system to verify that it is working correctly
- Notify patients when their information has been corrupt to allow them to help in the process of rectifying incorrect information.

#### Med-P02 Interview Transcript:

*Laura: So what if the Dentrex system were to crash, or have a problem, is there a number you can call?*

*PQ1: A support system, yeah. And that actually happened and I lost a lot of information. And I kept a backup as far as accounts, and it was only on the accounts receivable. So I did know that, but I didn't know anything else. So slowly we put it all back in through the hard copy, the files in there, we put the information back in. Worked a lot of weekends.*

*Laura: So do you keep a backup now?*

*PQ1: Yes, he does. He keeps it and takes it home every night.*

*Laurian: So it's done daily?*

*PQ1: Yes. And actually when it crashed I thought that I was actually backing it up and taking it home but the backup system hadn't been working for like 3 weeks and I didn't know it. So an electrical storm kind of took all of that out.*

#### Med-P03 Interview Transcript:

*Laura: .... Have you ever had problems like a crash?*

*PF1: Yeah. We actually lost a lot of account notes- we evidently had a virus attack it, and destroyed a lot of patient and account information. So now every day we have to do a backup and we print out hard copies of everything now. We lost about 3 years of information. So we at least keep our fingers crossed.*

Child-P03 Interview Transcript:

*PP1: And of course that's on our computer screen so we don't have to go to the hard file and pull it out. But it is duplicate information cause there is a hard file for everything that's in the electronic file. In case something happens to that electronic file, we do have the hard copy.*

### **9.50 Electronic Record Systems Crashing & Loosing Client Information (and Fears) (Study 2)**

Observed:

- Child-P06 2010-09-15 12:23PM
- Child-P06 2010-09-15 12:25PM

Within childcares there were not any instances of a computer crashing and losing client information, but there was a case of the Department of Social Service's computers contracting and spreading a virus. I searched for any news story to corroborate this story and there was nothing in any newspaper that I was able to locate. The way that PE1 from Child-P06 explained it to me, the inspector from the DSS came by earlier in the week to do her annual unannounced inspection. This inspection was unusual because the PD1, the inspector, reported that the DSS IT system was down because of a large computer virus that has spread from the Virginia DMV to the Virginia Department of Social Services. Because of this virus, PD1 had to do her inspection by hand and could not rely on any of her old notes about what the center was supposed to work on. Instead she had to ask for a copy of the prior inspection and had to do more work to verify that everything was in order.

Some salient points to highlight from these examples is that paper records serve and continue to serve as a valuable back-up for unreliable electronic systems. This duplication of information means twice the work to do along with twice the information to store and secure. The second is the invisible work of electronic system that results in an inability to determine if they are still working correctly. PQ1 would have been fine when the electronic system crashed had the back-up system been working correctly. Because she was not able to determine if it was working correctly, her time was lost. The third is that clients have little knowledge of when a crash like this has occurred.

PE1 from Child-P06 explained it best. She explained that in general she believes that she is pretty technically literate, but she fully acknowledges that her system is mostly paper. She says this is because if she leaves for the day, when she comes back in the morning she can "trust" that the paper will be there. She says that if she relied only on an electronic version she is not sure that over night her computer may "get a virus" and they she would have to spend time recovering the information from the parents again. She says that she does not know that the files are not also corrupt even if the computer virus was not as wide spread and then transfer the virus to any new computer as well. Instead she knows that the paper is going to be there and that she can access it and hand it to people. She says that she cannot trust the "security and longevity" of the computer to manage everything for her. She says also, that when parents come in and she needs to pull something up on the computer, she knows that the computer is going to act slowly.

With paper, she can put it in their hands straight away. With the computer she feels like they are just looking over her shoulder and the computer isn't doing anything.

From an activity theory standpoint this breakdown is simple: tool support was inadequate. Social systems have started duplicating work to prevent such critical breakdowns from happening again. Future designs should support making the back-up process more visible for clients, and support sharing this information with clients.

#### Design Implications:

- Present a visualization of the back-up process to care workers so that they can see whether back-ups have been successful.
- Periodically force care workers to access files from the back-up system to verify that it is working correctly
- Notify patients when their information has been corrupt to allow them to help in the process of rectifying incorrect information.

#### Child-P06 Observation Notes:

*2010-09-15 12:23PM She says that she believes that she is pretty technically literate, but she fully acknowledges that her system is mostly paper. She says this is because if she leaves for the day, when she comes back in the morning she can "trust" that the paper will be there. She doesn't know that over night she might get a virus on her computer and then have to spend all that time recovering the information and getting it from the parents again. She doesn't know that the files wouldn't also be corrupt and transfer the virus to any new computer as well. Instead she knows that the paper is going to be there and that she can access it and hand it to people. She says that she cannot trust the "security and longevity" of the computer to manage everything for her. She says also, that when parents come in and she needs to pull something up on the computer, she knows that the computer is going to act slow. With paper, she can put it in their hands straight away. With the computer she feels like they are just looking over her shoulder and the computer isn't doing anything.*

*2010-09-15 12:25PM She also talks about how the childcare was inspected last Tuesday. I wonder to myself why she didn't tell me this. She said it was really interesting because it was much different from how it is normally done since the state has gone paperless. Apparently the computer virus that took down all the DMV computers statewide affected more than just the DMV but spread to many other technical systems across the state. One of those systems was the Virginia Childcare Licensing. PE1, her licensor, had to do many things with paper and not with her computer. For instance, PE1 had to pull down their last inspection record and make a copy for PE1 to go through. She also had to make copies of other records for PE3 to take on paper, which she wouldn't have done previously. PE3 also told her not to access the*

*computer system online. She says that it will only hinder things right now since the system isn't working too well just yet - she doesn't need more people going on there and accessing it - which I found strange.*

### **9.51 Not Providing “Necessary” Information (SSN) (Study 1)**

Interview:

- Med-P07
- Med-P13
- Parent-P18

When a patient first joins a physician's office there is certain information that is requested by the practice. This includes prior medical history, insurance information, information about the current malady. It also includes collecting information such as the patient's social security number. From what can be gathered from interviews and observations there are two purposes for collecting a patient's social security number. (Social security numbers are particularly highlighted because it is a primary indicator of identity and can be stolen.) The first reason is because it is used by some insurance companies as the primary key for locating the patient's policy information. For instance, two practices were observed looking up a patient's insurance policy through an insurance website (cannot look up website because you have to be logged in as a provider before you can look up a patient's "EOB": Explanation of Benefits). The patient's social security number can be used here to locate the patient's information and verify that they have the correct person. The second reason is because the office cannot reclaim lost pay through a collections agency unless they have the client's social security number. Given these purposes, the physicians' offices that were interviewed and observed attempted to collect all client's social security numbers

There were two physician's office directors who discussed instances where they do not force their clients to provide their social security number. Given the risk of a client's social security number being disclosed, some patients do not desire to provide that information. The question then arises for how does the negotiation between providing and not providing a social security number resolve. In the two cases that were discussed for physician's offices, the office made exceptions for those people. One or two people out of the hundreds or thousands of people who are seen does not make a large impact on the business side of the office, it would be assumed.

In these breakdowns, what is highlighted is that the office may be trusted with providing adequate care, but they are not trusted to manage the client's sensitive personal information. Therefore, clients try to find additional methods of completing the objective of their activity, adequate care, without having to also compromise on the activity of protecting their sensitive personal information.

Design Implications:

- Support layered security protocols for accessing degrees of private information. For instance, before accessing a patient's social security number the care provider has to uniquely log-in and a notification is sent to the client; versus, accessing a

- patient's x-ray which holds no personally identifying information has an access log that is not checked as often.
- Support the patient being able to see who and when personal information was accessed and used to help build trust between client and care provider.

Med-P07 Interview Transcript:

*Laura: Do you get a social security number from everybody or just for insurance?*

*PA3: We try to get a social from everybody, but every now and then, like if it's a child and the parents don't know it, we don't worry about it. We'll let it slide.*

Med-P13 Interview Transcript:

*Laura: So do you get a social security number from every patient that comes in?*

*PN1: Every patient, yeah.*

*PN2: We had 2 that didn't want to supply a social security number.*

*Laura: And that was okay as far as...*

*PN1: So far it seems okay. We had to call the insurance company and explain to them and get them to go ahead and go alright. It seemed to go. But they won't accept a claim electronically right of the bat with a social security number missing.*

Parent-P18 Interview Transcript:

*Zalia: So, when you decided not to give or put your son's social security number on that did they say something else may be... say any other identity that may be used in place of that?*

*Participant18: No if I recall correctly, every time I handed in those forms at the daycares I say 'I don't know their' or 'I don't have their social security number's and they like said "alright don't worry about it". So.*

### **9.52 Hesitation About Writing/Storing Client Information (Suspected Abuse) (Study 1)**

Observed:

- Child-P03 2009-10-21 10:35AM

Interview:

- Med-P07
- Med-P08
- Med-P09
- Med-P12
- Child-P01
- Child-P04 (2 instances)
- Child-P06
- Child-P07 (2 instances)

As discussed in previous breakdown themes (e.g., Knowing a Patient's Private circumstances), there is information about a patient that is useful for the care of the patient, but is not directly related to the care that is being provided. Examples from the interviews below include patient concerns over procedures, worries that a patient may have about the facilities, of the patient has an unrelated medical issue such as Alzheimer's, or if the patient's behavior is obnoxious or sporadic.

There are concerns, though, for how to manage documenting these issues. As the director from Med-P12 discusses, if something is placed in a patient's file, and then the file is subpoenaed, the doctor can be liable for what is written in that file. If what is written in the file is a little contentious, it can become a serious issue for the health care worker. This means that the health care workers have to be careful about what is documented, even though they are encouraged to write everything down (e.g., PG1 from Med-P04 said, "So even if it's taboo, of course we train our doctors to write it all down, write it all down. So that way you can always say look we dealt with it appropriately. What you can't do is if you don't do that... we always teach our doctors that you gotta look at, if we're in the court of law, can you explain what you did. And if you write it down then you got a record of what occurred.")

To deal with these conflicting issues of needing to protect your rights by writing everything down, but not writing everything that is contentious, the health care workers are dealing with conflicting activities. They need to be able to manage their privacy needs of making sure that contentious information being documented about a patient is not passed on, but at the same time managing the care of that patient in a reasonable manner. As discussed by two of the quotations below, post-it notes are used to provide meta-information about the patient that may be valuable. Post-its serve as a temporary meta-information that can be stored for the length of the issue, can be easily discarded, and are also easily identifiable for relaying information. For this reason, they are employed to balance these conflicting activity objectives.

Childcare centers have similar concerns about not wanting to document everything about a child and their family. A reason provided for this is because of the free access to information in the childcare center. For instance, the director from Child-P07 explains that even though she attempts to restrict access to who accesses a file by going through her, she does not want to label the child or provide a way for people to find out unnecessary information. Because of this, there can be knowledge about a child that is "implicit". Examples include if a child is difficult, marital problems between the child's parents, and the identity of a child's parents (e.g., that's not *really* dad). The ambiguity over this information allows for personnel to negotiate the formalized need for documentation while respecting the necessity for nebulous situations.

A second reason for being hesitant for documenting about a child is in cases of abuse. Childcare center personnel explain that they are "mandatory reporters", meaning that if they suspect child abuse, they are mandated to report the evidence to higher law-enforcing agencies. The hesitation is due to the serious ramifications of the allegations being true. A child coming in dirty once can perhaps be an anomaly, but once someone

believes that there is possible repeated evidence, the childcare starts to document this evidence. When the childcare believes there is sufficient evidence, then they will turn over the evidence to someone in the department of child services. Up until that point, though, there is hesitation over whether or not to document these cases, and if they do document, how to do so in a way that respects the privacy of the situation.

Design Implications:

- Support meta-layering information that cannot be subpoenaed.
- Support decaying client information that will not be stored, but can be linked to client information
- Provide the ability to store information about a client that is not strictly medical information but is relevant to the care of that patient.
- Provide a place to document issues related to child abuse

Child-P03 Observation Notes:

*2009-10-21 10:35AM PP2 tells me that teachers have a confidential log that they keep to monitor any suspicious activity, bruises, bumps or anything that the kid says that indicates something is wrong. They also list temperature in case of fever or so. In such case, where the child is sick and a log is kept, it is not shared with the parent. The parent only gets a form indicating the sickness and how long the child should be symptom free before coming back to the center.*

Med-P07 Interview Transcript:

*Laura: Okay, is there ever any information that people might be hesitant to write down about a patient? Like in their chart.*

*PA3: Personal-wise you mean... meaning if they're like...mental stuff?*

*Laura: Right*

*Laurian: Can you give us an example of a particular case?*

*PA3: Like if somebody is talking about, like everything they're saying isn't making any sense, or they're bouncing back and forth, you know, stuff that doesn't have anything to do with their eyes but that we'd want to let the doctor know. Or if we're not sure if they're. Sometimes Alzheimer's patients can be really tough.*

Med-P08 Interview Transcript:

*Laurian: Okay and just to follow up on the question about anything you wouldn't write down, is there anything you wouldn't put in a patient's file but that you might know about a particular patient?*

*Laura: Like one example that I can think of would be if somebody came in and they were just belligerent...*

*PII: Oh, yeah, sometimes we'll just let the doctor know if somebody's having problems like that we'll stick a post-it note on the front of the chart just to give him a heads up, and then we'll shred it, like we've had a couple people fuss about the handicap ramp, it's not so good, but he's working on that. But we'll let him know, you know, say something to the*

*doctor, put a note on there just to give him a head's up that they may say something. That kind of thing.*

Med-P09 Interview Transcript:

*Laura: Is there ever information that you might be hesitant to write down on a patient's chart? Like if someone is real belligerent or talking to themselves? That doesn't necessarily have to do with their eye health, but that you'd want the doctor to know?*

*PT2: Well we don't write it down in the chart per se. We put it on a little post it note so that he can be aware.*

Med-P12 Interview Transcript:

*Laura: Is there ever information that you wouldn't write down that you might know about a patient? Like say they're belligerent or have a mental disorder that may not be relevant to their direct medical care, but may be relevant as far as interacting with them?*

*Dr D: Yeah you don't write down everything. I mean if a patient, I mean, we intermittently will have patients who are very difficult to get along with. Either they're scared to death or they're just obnoxious to start with. Or whatever. Sometimes you write that down in the chart, sometimes you don't. Sometimes, and there are all shades of gray... but usually if it's really an obnoxiousness or a form of behavior that would be good for someone to know in the future who may have to deal with this patient, then we'll write it down. But people tend to soften it quite a bit. Because you don't want to write something down and then be looked at, you know, and someone will say, or if a lawyer looks at it, "well I guess you didn't like your patient did you?" So you gotta be objective about it and not let your feelings come through. But it's sometimes helpful to write down behavioral issues.*

...

*Dr D: Yes they have access to everything in their own chart. Of course they can show it to the lawyer, and then the lawyer will send it to a doctor that he employs, usually, to look at it, and then he'll give an opinion as to whether he thinks the care is up to standard or not. So that's one of many reasons why you need to be discreet about what you write in a file.*

ChildP01 Interview Transcript:

*Laurian: "And how, does the file get used in that situation?"*

*Interviewee: "The file doesn't really get used in that situation. It's more teacher-documented activity. When we have a concern about child--if it's child abuse, if it's developmental, we start kind of documenting, you know 'on such and such date, this is what happened, this is what the child said, or what he's not doing, or what he's doing too much of' if he's overly aggressive and assertive. And so, they keep that, they use initials, they put it in a cabinet up and away so that no one will accidentally discover it, where only the teachers know where it is. And, then when we have a*

*conference with the parents, we can kinda sit down using that information as a tool and say 'well, these are some of the things we've seen for example on these days, it's not just a one time experience we've seen, we're starting to see a pattern' and so it becomes more of a tool than it becomes a form."*

...

*Interviewee: "Noooo, but. It's again, when it comes down to reporting a case of abuse or neglect, I mean, it's hard when we're collecting information. We have to act pretty quickly, but at the same time we don't want them to see, like especially if it becomes an unfounded case--be like 'why are you collecting this information, you're saying I'm a bad parent'--so, we try to keep that stuff kinda separate and aside and away so that it's not necessarily 100% visible. If it doesn't come to fruition, if licensing does step in or social services steps in, you know, then it becomes a more prominent feature, because obviously they know about it. But, it's a tricky line, you know, the owner and I were talking about it not so long ago. It's scary for us because you never know how a parent's gonna react and technically we're supposed to go to Social Services before we go to a parent, but you know what if there's a case where you know, you know family strife is going on, and it's very stressful right now, and what is the real story--is it a matter of frustration at the moment. You know was it a one time thing and so what's the right thing to do--really go to Social Services and risk the child being yanked from the classrooms, their home life, and an already stressful environment that will move on and be happier. Or, you know, go to the families first and say 'hey, we're noticing things and we're concerned for your family. But, really we do try to keep that kinda separate until things are discussed."*

...

*Interviewee: "If we're collecting information on a possible abuse, or a possible developmental thing, that's kinda kept up and away so that we can finish collecting it. We don't want parents to get upset and overwrought and then skew things out of proportion"*

#### Child-P06 Interview Transcript:

*P6: yeah, that's a good point... we're mandated reporters which means that if we suspect abuse then we report it by law and we can be held liable if we don't... and so the sticky thing about calling the department of social services is that you want the child's best interest but you set a ball rolling that is not to be stopped once you call, so you do want to make sure that you are pretty confident about calling... I mean I wouldn't hesitate to do it if there was a risk but you do kind of make sure... so we might put in the file documentation, or a file to state we had these concerns about things a child said... in the past we've seen if a child drew a picture or something that was concerning then we might stick that in there and not disclose that to the parent partly because my experience has been that if you bring that to a parent at a point - they would be happy for you bringing it up and so*

*sometimes it's a conversation better left to authorities... if you're really concerned, I mean small things we'd encourage staff to bring it to the parent's attention but if it was more serious those kind of things we might [report]...*

Child-P04 Interview Transcript:

*Interviewee: "On a daily basis, PU3, our program assistant will go to each classroom by 9:30 to ask the teachers 'who's not here that you're anticipating?' A lot of--the parents are really good about saying 'we're gonna take a trip tomorrow, he won't be here' so the teachers will say, well, these three children are out but we knew about it, but this one we haven't heard from, and they're not here yet. So, those are the ones that PU3 will call to follow-up. And, she does document who's not here on a daily basis, as well as--you know, if we had to make a phone call, what their reason was. And, we do that--for a lot of reasons, just to make sure that a child hasn't been left in a car, something like that--just to make sure something that could be potentially harmful hasn't happened. And, to make sure--ratio-wise*

*Stacy: "I've heard of situations where there might be--if there might be a case of abuse, you might see some signs on the child that make you think it could be an abuse situation, maybe you would document some of that sort of to yourself but you wouldn't share that with the parents until you've gathered information enough to either talk to the parents about it or talk to social services about it. I wonder where you document that information and where it is kept."*

*Interviewee: "It's kept in my office, in a file. And, I just have it kind of tucked away and there have been a couple instances where we've, you know it's usually just teacher's notes--their dictation of something a child has said--just so that we, you know, it's not enough--we are mandated reporters--not enough that we report, but we want to see if there's a pattern that's established or if a child--you know, sometimes they just--"*

*Stacy: "--bumpin' into things--"*

*Interviewee: "--say things. There was one time we documented something, and I did follow up with the parent and she told me what had happened, so we just made a note of that. So, we do have one of those little file folders, and it's in a locked, secure location."*

*Stacy: "So, it's not in the file with all the other children's information?"*

*Interviewee: "I don't keep it in the child's file, no, it's in a separate file, just at the very back."*

*Stacy: "OK, in the back of this cabinet?"*

*Interviewee: "Yeah, the very back"*

Child-P07 Interview Transcript:

*Tom: another thing that I've heard before is, if you've had a conversation with a parent and noticed maybe a risk factor you'd jot that down in the file or something*

*P7: i don't, no... I maybe keep it in my personal information just as a reminder to myself but I don't put it in the file because the teachers can access their kids - and kind of the same thing like not wanting to label the child as inflicting a certain kind of injury on someone, I don't want to necessarily want to label a parent for everybody and I'd rather - if there's something going on with the child i know about I'd rather hear maybe from the teacher in an impartial way, you know, if "this person is doing this or that" i might - well that could be related to, so... instead of giving them something to necessarily look for because then you might find it*

*Tom: i think that cover pretty much all of the table...one question I haven't asked yet I wanted to ask you... could you think of any information that everyone sort of knows but don't record?*

*P7: yes... family situations... a lot of the times we'll have a listing like the father listed, the mother listed, work phone numbers, place of employment... and sometimes we'll have the same address for them listed but yet it will be understood around the center that they're not together... they're either separated, in the progress of getting separated, they've never been married - a lot of the times family situations is definitely an implicit - and we kind of have a lot of convoluted family situations... and a lot of the times we will have a person listed as the child's father but is not actually the child's father and we know that but it's not, you know, listed in there as known... and so that would be - and i don't know if it's like that in other centers, like I said, we are one of the only centers in the area that takes DSS stipends so we do have kind of a unique population that way... so that might be piece of implicit information we do have that we know is not necessarily- and sometimes, you know, the parents don't want to put it down in writing.. it's a dynamic situation, you know, it's not set in stone... [tangent] and I guess you know, the personally quirks about the kids - it's not written down anywhere but, you know, we get to know the kids and we get to know, you know, "this one throws a temper tantrum like clockwork every Thursday before naptime" or, you know, "if you take the blue stick away from this one he will go ape on you"... we don't write it down but we know - we know the kids and we know which ones are easy to get along with and which ones just aren't.. and for as many kids as we have we still know all the kids and people get a pretty good eye on which kids are like that... that's definitely implicit information, you never write that kind of stuff down, you just don't - I actually have my degree in elementary ed and that was one thing they always told us, you know, not to keep notes on kids that are difficult because if you have it written down somewhere in a file or something it could eventually get to somebody else and then you have stuck this kid with a label that may not be true a year from now, or a month from now, especially in this age group, so..*

### **9.53 Lost Paper Patient File (Study 1)**

Interview:

- Med-P10

Similar to the theme ‘Difficulty Locating Patient File’, this breakdown actually discusses a patient file being lost. Med-P10 was the only office that had no electronic system to back up all of his paper files. Therefore, if the paper file was lost there was not a secondary supplemental record to serve as a back-up for the lost paper file. This lack of a back-up for the paper files may seem a little archaic given the growing model of repeatable backing up and storing old back-ups of business information. The inability to back-up client’s files, nor the apparent lack of concern surrounding what happens when a patient’s file is lost are indicators of the value that is placed on that information. When a health care worker is constantly managing sensitive personal information they can become innocuous to the value of that information.

What is also important from this one quotation is what is missing from it. He does not mention letting the patient know that the file was lost. He does not mention reporting the lost information, or how he goes about recreating the file.

Design Implications:

- Support backing up paper records
- Support notification of patients when their information is lost

P10 Interview Transcript:

*Laura: All right, has there ever been a time when somebody’s information got lost?*

*PL1: It gets mis-filed occasionally.*

*Laura: So are they filed in alphabetical order?*

*PL1: Yes*

*Laurian: What happens when a file is mis-filed?*

*PL1: Well the first thing we do is look for them. They will occasionally stick together, and sometimes you just don’t find it. I will then re-create the file.*

### **9.54 “Inappropriate” Staff Access of Client Information (Study 1)**

Interview:

- Med-P12

Sensitive personal information about a client is stored inside a client’s file. At most locations, this information is not kept very secure: passwords are not used, passwords are shared, files are left out in the open, and client information is freely discussed by the staff. Some places, though, do have ways to audit who has accessed a client file to review whether privacy policies have been followed by the staff. When a client’s file is reviewed, a log of who has accessed that file, and when can be seen and somehow privacy breaches are detected.

While these instances were never observed, one participant did discuss that he knew of instances where people were fired because they had looked at information that they should not have. The cases he cited were where a nurse or doctor was looking at family members' information. While this may appear innocuous, it is against the privacy policies of the hospital. And, with a hospital filled with 4,000 employees, the sheer amount of data that is available to the staff is huge that can serve as temptation.

From an Activity Theory standpoint the staff that examines client information that they should not look at are breaking a rule, or a social norm, that governs the relationship between subject and community. Whereas in other cases listed in this appendix demonstrate places where rules are not known, this example demonstrates a place in the socio-technical system where an explicit rule was not followed.

Design Implications:

- Auditing audit trails takes manpower. One method to decrease the need for people hired by the office to audit records is for a patient to be able to see who has accessed their file and to raise questions when necessary.
- Use physical tracking of people within proximity of a patient to create a general schema of people who would “normally” be allowed to see the patient's file. Flag others as possibly inappropriate.

Med-P12 Interview Transcript:

*Dr D: No. Well they say that, for example, they intermittently will check to see people logging into other people with the same name. So to make sure that the nurses and doctors aren't looking at their family members' information. And intermittently they'll pull a log and make sure that everybody was looking where they were supposed to be. But as you can imagine it's such a huge system it's really hard to keep close track of it.*

*Laura: Have you ever heard of a time when somebody was doing that?*

*Dr D: Yeah I've heard that, I mean, there are 4000 employees of Centra health. But I have heard that people have gotten fired- I mean, they tell the nurses and doctors, but the doctors are for the most part not employees of the hospital. But they tell the hospital employees that if you're caught looking at the wrong chart, you're fired. And I've heard of a couple of times in the last 5 years where that's actually happened. The nurses I have to say are very skittish about that. Making sure they don't access or look at something they're not supposed to look at. And they don't. It's really, because of the seriousness of it, it's really taken very seriously. Now this, this is different. To look at the schedule, anybody who knows the username and password can, it's just one. But in order to get in and look at patient records you have to have a username and password that's individual, that's linked to me and to any other individual here.*

### **9.55 Client's Family/Friend/Neighbors Discussing Client Information (Study 1)**

Observed:

- Child-P03 2009-09-15 3:23PM

Interview:

- Med-P02
- Med-P12

Patients do not live in a glass box. Their community and their family work to support them when they are in need of medical care. These people help those who are in care by managing communication with health care workers, and working as a buffer. For instance, patients can feel overwhelmed by the amount of information being told to them about their medical condition, and a friend and colleague can support that person by asking important questions. Or, when a patient is medically incapacitated, the friend or family member can contact the health care worker to relay information. These community members serve a valuable role in maintaining the care of the patient. The problem is that, for the family or friend to legally be allowed to discuss information about the patient, the patient has to have signed a form stating that they give permission. What happens, though, when there is not a form that is signed? How do the offices deal with this issue?

In the two quotations from interviews of medical directors below illustrate two different examples of dealing with this tension, and they illustrate a place where at one health care worker admitted that there are times when he has an “understanding” but makes no reference to having paperwork signed. To contrast that example, though, there are times when a physician’s office has had to protect client information. In the first example PQ1 from Med-P01 discusses how she has learned not to just tell anyone about a patient’s medical information. She says that she realizes that there are cases where former spouses try and gain contact to one another through second parties like a physician’s office. While she has never knowingly encountered that kind of situation, she has had situations where a grandmother wanted to pay for the child’s exams. She has had to defer grandmothers away from being able to access even payment information about the client.

In the second interview example, Dr. D from Med-P12 explains how he receives calls from his patient’s children asking questions about their parent’s medical procedure. Dr. D explains that he generates an “understanding” with these people, because “often” it is someone that he has had contact with previously. Given the number of patients he sees though, and the ability to recall that kind of information from memory, it seems hard to believe that he would be able to recall every patient’s family member who he should or should not deal with. This quotation also does not mention that he checks to see if the parent has signed any forms allowing their children to discuss their medical history.

Childcares are also highly social spaces that are in part about the social relationship that children are forming to one another. For this reason parents call each other, join PTAs, and invite each other’s children over for play dates. While all the childcares reported that they respected the privacy of their clients, there were childcares that provided places for parents to communicate with one another such as listservs and providing a parent phone directory. There was one instance that was observed at Child-P03 where there is no PTA

or parent directory, when one parent asked for the phone number of another. PP1, the director, worked to provide this information without checking with the parent.

The point of these examples is not to demonstrate how information was leaked or privacy was breached. Instead, it is to demonstrate a place where even the current system does not support the shifting landscape of social relationships. It would be better to design a system where a patient can verify after the fact who has been discussing their information, or to provide some shifting lightweight method of allowing a person to be allowed access to a patient's information.

The breakdown in this case exists because the patient's privacy is not being protected in all cases, and in some cases the activity of providing and sharing a patient's care are not being properly managed. While the rules are clear (e.g., do not share a client's private information with external people), this activity is not necessarily in congruence with the activity of managing a patient's care, thus resulting in a breakdown.

#### Design Implications:

- Allow for decaying access to sharing information.
- Provide additional means for a family member or friend to access patient information without having explicit HIPAA access.
- Provide a lightweight mechanism for checking if a person has access to a patient's information.

#### Child-P03 Observation Notes:

*2009-10-15 3:23PM PP1 is looking at her computer monitor and typing something. A little later she turns to PP2 and says that one parent asked about contact information of a child who was in the same class with their child. PP1 trying to remember the name of the other child the parents told her. She is confused whether it was Name1 or Name2. There is multiple Isabel but one Annabel who does not seem to belong to the same class where the child of the asking parent goes. PP2 is also confused and agrees that there is one Name2 in this center. PP1 says she may need to talk to the parent again to get the correct name.*

#### Med-P02 Interview Transcript:

*PQ1: If the parent has signed the HIPAA, then that would tell me who can or cannot get the information... You know as time goes you learn you pretty much learn just to tell the patient, because you could get an ex-wife who calls herself the wife, or...*

*Laurian: Has there ever been a case of that?*

*PQ1: No, but I'm trying to think. Nothing as far as marriage, but I have had mothers who say if my mom calls, don't tell her. Grandmas are probably the worst. They want to take care of, or pay for it. Some parents don't like that. So if they want to pay for it they have to give it to the parent.*

Med-P12 Interview Transcript:

*Laura: Do patient's families ever ask for patient information?*

*Dr D: Well my experience with that is that I do nerve blocks for people with back pain. I do epidural steroid injections for example. Often those folks are old, and lots of time one of their children will call in and say you know my 86-year-old mother you gave an epidural to last week. And I always tell them to call in a week and let me know how they're doing. So it's often a daughter or a son or sometimes it's a next-door neighbor. But it's always someone who you've had contact with before so there's an understanding that they have access to that information.*

### **9.56 Client's Family/Friend/Neighbors Discussing Client Information (Study 2)**

Observed:

- Med-P16 2010-08-19 3:12PM

In the example from the observation records, the PB1 from Med-P16 has explained a strange circumstance to her colleagues where a patient's husband was trying to locate her wife. The end result is that the message from the husband to the wife was relayed. However, this example illustrates how a nurse at the office asserted that this was a HIPAA violation. The mere fact that the patient was at the location is considered private information that should be protected but was not.

Design Implications:

- Provide some lightweight mechanism for people to verify who they are.
- Provide a way of documenting who calls and verifying later with the patient.

Med-P16 Observation Notes:

*2010-08-19 3:12PM Dr-PB3 comes in and PB1 talks about a phone call earlier. It was another office. It was a man who was looking for his wife and he thought that she was at the dentist. And so the place figured that the wife might be here. And sure enough the wife was at this location. So PB1 said that she would pass on the message to the wife - which was that he was at the garage across the street and needed picking up. The doctor said that that was good. But Nurse-3 said that was against HIPAA. The doctor jokes that Nurse-3 is all HIPAA compliant - he acts like he doesn't take it very seriously. She says, "Well, that is about privacy, what if he was an estranged spouse looking for his wife to kill her." And then they talk about people going on murdering sprees for a second. There isn't a conclusion on whether or not PB1 did the right thing.*

### **9.57 Doctors Exchanging Client Information (Study 1)**

Interview:

- Med-P12

There are times when a doctor only has a short amount of time to make a decision about what to do about a patient. For instance, Med-P12 discussed in his interview how there are times when he needs to quickly consult another doctor, who is not at his practice, about the results of a patient's test. There is not an infinite amount of time, and the patient needs to be seen about their current issue. This means that the doctor may have to seek an off-the-cuff consultation from another doctor, with or without the client's permission to share that information.

Med-P12 discusses in general how he handles these kinds of cases. He gives an example of a patient who came into his outpatient surgery center but was complaining of chest pains. Rather than cancel the surgery, he quickly calls his colleague or he will fax over the results from a test to get a consultation from that doctor. This allows the doctors to communicate in real time to get results that affect their schedule and the outcome of the patient's surgery. However, it also means that the patient's information is being sent to another office without the explicit permission from the client. While the client may prefer that the doctor receive this consultation rather than cancel the surgery, this does not mean that the patient's privacy should also not be maintained.

In this case, a breakdown occurs because the activity of completing a surgery is in conflict with the activity of maintaining patient privacy. Possible solutions would be to build in patient privacy into the actions of doing a quick consult so that they seamlessly support the action.

#### Design Implications:

- Support decaying patient information
- Support the patient's ability to identify what information they would like that physicians' offices to still have access to, with a default setting of opt-out after a set period of time.

#### Med-P12 Interview Transcript:

*Laura: Are you the one that's referred to?*

*Dr D: Yeah. But I often will call another doctor and say you know, I've got a patient here for surgery and he told me he had chest pain the other day. So they'll get a consult. Or if we get a pre-op EKG that looks a little funny to us, we'll often fax it to the cardiologist across the street. We'll often fax it over there and/or we'll call and say we have a patient with a question, will you look at the EKG.*

*Laura: when you do stuff like that do you have to worry about insurance or anything like that being involved? Like if the cardiologist across the street isn't on their HMO plan?*

*Dr D: Well they'll usually just look at it and give you, sort of an informal opinion, especially if it's their patient, they'll look at the EKG and go, okay, it's exactly like the one he had last week, or they'll say oh my god this is different, don't do the surgery, send him across the street right now, or tell him to set up an appointment in a week, or whatever depending on the seriousness of it.*

*Laurian: What patient information is on those things that get faxed?*  
*Dr D: The patient's name at the very least, and then sometimes the medical record number and the birth date. But that happens all the time. We fax patient information back and forth to offices. For example if they post a knee-scope on a patient, from the orthopedics next door, they'll send out the, fax it out from the office. That happens hundreds of times a day, there's always stuff getting faxed. Always with the big disclaimer this is medically protected information, and this is intended for so and so only.*

### **9.58 Receptionist Functioning as Nurse (Study 2)**

Observed:

- Med-P15 2010-07-01 9:43AM

The nature of small physicians' offices is that there is a lot of work to be done, and not many people around to do it. This means that nurses and doctors sometimes have to answer the phone, pull their own patient files, and do all kind of work that is not associated with their "role". For example, PS1, the director from Med-P19 says, "I don't really believe in job descriptions for that very reason, because everybody needs to do everything and know everything. That's the only way it can work in this day." This quotation reflects a general practice of these locations. Everyone lends a hand at whatever job is necessary for the function of the business. This leads to receptionist finding cases where doctors have prescribed a procedure that might kill their patient (Med-P15), doctors making copies of papers and collating them (Med-P16), and doctors delivering mail (Med-P17).

The breakdown in this situation occurs when people in the office do work that they are not allowed to do. This was only observed once, at Med-P15, where the receptionist is seen to be writing prescriptions for patients. A nurse sees this and while she does not take away the prescription pad, she reminds the receptionist that she is not supposed to be doing that. In this case, the breakdown occurs because the activity of collaborative tasking and a shared division of labor comes in conflict with the rules governing who can do what work.

Design Implications:

- Support shared jobs, but flag when someone completed a job outside of their job role for review

Med-P15 Observation Notes:

*2010-07-01 9:43 PC4 asks PC1: "Are you writing a prescription?" PC1 responds, "I am." I'm not sure why she was writing a prescription nor what prompted her to do so but PC4's tone sounded disapproving almost as if PC1 wasn't supposed to be writing prescriptions.*

### **9.59 Fields Not Providing Enough Patient Information (Study 2)**

Observed:

- Med-P16 2010-07-13 2:36PM

Physicians' offices document the procedures that were conducted on patients by using codes that are associated with various pieces of metadata (e.g., cost of procedure). All offices used some kind of billing software that involved entering these codes so that they could submit the bills to various electronic insurance filing systems. There is not much of a way to get around using these codes. The problem is that they can be very reductive, and can abstract too far away from what was actually done with the patient.

In particular, both the office staff and the doctor at Med-P16 discussed separately how they use additional means to convey what happened with a patient. They write letters that explain what is wrong with the patient that are a couple of paragraphs long. The codes are still included in the letter, for other practices that may want to use that as well, but the long explanation is combined for "accuracy." The doctor describes his method below in the observation notes: hand writing malady, treatments, and stickers for drugs, dosages, letter writing, etc.

The breakdown occurs here because the participants do not believe that the system provides a rich enough medium to capture patient issues. Because it does not support collecting that information, supplemental information collection and dissemination systems have been created that display client information in additional, and possibly less secure mediums.

#### Design Implications:

- Support using codes, but also facilitating when the doctor wants to associate more information with those codes – such as what they mean in this particular instance.
- Support transferring codes and their entered meta-information into additional formats such as letters.

#### Med-P16 Observation Notes:

*2010-07-13 2:36PM (Tom's Notes) First off he writes on particular piece of paper to explain the reason for the visit and any immediate treatment that he administered. Then he has sheets of stickers with drugs and dosages printed up so he can stick them to these papers. These "letters" as he calls them are prepared for dictation so that other doctors can receive them. Dr-PB3 expresses his disdain for "fields." He says that he'd rather write a paragraph or two on each letter, attach the stickers, then send them out after typed up. Predetermined fields on his letters are not as accurate he says. After he finishes writing these letters they are typed up by PB2. She can type up to 40 letters a week and uses 'shortcuts' (he did not elaborate as what these are) to do so.*

*2010-07-13 2:35P.M (Aubrey's Notes) PB1 takes two papers down off of the wall to her left and back. She writes on them, and then sticks them back up. She teaks them down and back up again. She types into the digital calendar and PB2 walks in. They tell us that they put scheduling into this system, but not procedure notes. They also describe medications.*

*PB1 puts two stickers on the file that are the size of address labels with words & blank lines. PB1 tells us how they write their letters individually so she can preserve what she does accurately. She says that they don't use forms and write between five and twenty letters a day, four days a week. She explains that field letters don't work, for whatever reason.*

### **9.60 Patients Not Recognizing Updated Information (Study 2)**

Observed:

- Med-P16 2010-07-13 3:37PM

When a patient enters the physicians' offices, they can be asked to re-fill out patient information sheets, even though there are identical sheets already in the patient's file. This is because there are times when there has been an extended period of time between the previous visit to the practice and the current visit. Even though the patient may assert that no information has changed (e.g., that they live in the same location and their phone number is the same), the practice gives the patient this sheet just to make sure. Handing over these sheets was observed in every physician's office. An excerpt from observation notes below from Med-P16 is included, because PB1 asserts that even though people say nothing has changed, she believes that information actually has.

In this case, we have a system where physician's office staff have created a method where patients verify their information. This allows the office to establish that their information is up to date.

The breakdown occurs here because the office does not trust the patient that their information is up to date. This is one symptom of how patients do not have a way to verify their information, and an easy way for the two parties to share what information is being managed. This breakdown affects the trust between the two parties, and can be possibly solved with modifying the patient's agency in managing her information.

Design Implications:

- Create a way for offices to verify patient information that does not result in testing the patients.

Med-P16 Observation Notes:

*2010-07-13 3:37PM She gives him an update information sheet. She tells me that often people say nothing has changed, when things actually have.*

### **9.61 Sharing Login (Study 1)**

Observation:

- Child-P06 2009-10-22 1:48PM

Interview:

- Child-P12

In childcares there was two childcares that use web camera systems. One of these kept digital archives of the videos that required password use. However, there was only one

password for accessing the system and it was shared between the three administrators from Child-P03. What is interesting about Child-P03 is that it is the only place that reports using individual passwords for their electronic record keeping system. It makes me believe that in the case of the digital archive the system does not support numerous passwords rather than the people opting to not use individual passwords.

This breakdown is a result of a lack of adequate tool support along with a lack of enforcing the objective of maintaining a trail of who has accessed the video data.

Design Implications:

- Support additional methods of logging into the computer – such as location detection

Child-P06 Observation Notes:

*2009-10-22 1:48PM The lead teacher in the lobby computer asks PE1 about the password of the computer. This is what she said, 'Hey PE1, eventually I will remember the password, but can you tell me now'. PE1 gives out the password loudly. Anyone in the office or lobby or infant room should be able to hear it. It's a sequence of four digits like 1234.*

Child-P12 Interview Transcript:

*Tom: ok, and what kind of policies are there with the information... I'm guessing it's recorded?*

*P12: yeah, this streams into DVR which is recorded and the parents have access to it and they're the only ones who have access to it... Rhonda has an administrator and the owners do as an administrator - they have an administrator password... so everyone has a username and password that's specific to their child... the rooms that are available are specific to their children*

## **9.62 Sharing Login(Study 2)**

Observed:

- Med-P17 2010-07-15 11:18-11:27AM

Interview:

- Med-P19

It was documented in another breakdown theme that childcares and physicians' offices can have systems that in general do not use or require passwords. This theme is different in that there are places that do have passwords, and have individual passwords. However, even in these cases, their use still does not follow the traditional model of one person using one password. As can be seen from the examples below, this is because even though password use is important, it still does not fit in with the flexible work of these centers.

For instance, in the first example, at Med-P17, PA4 needs to get information from another database of patient information at the hospital. The problem is that she does not

have access to that database with her information. She knows that she needs to go through whatever procedure is required for that process, but states that “she’s working on getting access to the system.” Until she receives access, she has to use PA7’s password and login to the hospital system. This is acquired by starting to log into the hospital system, and then asking PA7 to log in for her. This system of borrowing log in information allows the practice to share in the work that has to be done, and also the *responsibility* and *accountability* of the work.

In the second example, PS1 from Med-P19 discusses with Aubrey and Tom how everyone in the practice has individual passwords. People will log into their computers and use that login all day. PS1 explains, though, that people will use another’s machine that another person has logged into. This is because everyone in the office “has the same access” and “there is no really privacy act between employees.” She means that everyone has permission to see the same information. Because everyone has the same permission, there is not a need to have an explicit rule specifying that they can or cannot use each other’s computer. This fact is inherent in the work that they do and the information that they are all allowed to see/access/modify.

From an Activity Theory analysis, the activity of handling patient care is in conflict with the activity of using individual passwords. The objective of using a password to log who is doing what is obscured by the fact that there is no visible outcome. The objective of client privacy is not fulfilled by the activity of individually logging on. For this reason, the staff does not do this activity.

#### Design Implications:

- Supported layered logins – one for the person who logged in first thing in the morning and one for the person who currently wants to use the system
- Support additional methods of logging into the computer – such as location detection

#### Med-P17 Observation Notes:

*2010-05-15 11:18AM PA4 tells me another random fact: when she enters newborns into the system their first names are not always permanent. At this point I think PA4 is entering some of the newborns into the system since she goes to asks PA7 to sign her into the Montgomery Regional hospital system. PA7 says that she needs to get her key fob and returns moments later with it in hand. She goes to a webpage saved in her favorites, and enters the code generated by the device. She clicks on a link located on this site and it launches a smaller window that looks like a small terminal window. In this blue terminal she has to enter a username and password which she types from memory this time. The final screen says "Office Billing Menu". She gets up and lets PA4 get back to work. 11:27AM She tells me that she's on Montgomery Regional Hospital's system in order to look up their procedure codes. I think that the demographic sheets that she receives from the hospital don't actually say the procedure that happened instead they provide numerical codes. To*

*enter the procedures into e-MDs PA4 needs to find out what the procedure codes mean. She mentions that she's working on getting access to the system but uses PA7's for now.*

Med-P19 Interview Transcript:

*Aubrey: Okay, so when you sit down at the computer you log in, do what you do, and then you would log back out immediately or?*

*PS1: That depends. Sometimes we leave them logged in all day depending on how busy we are and what we are doing.*

*Aubrey: Okay.*

*PS1: So there is no really privacy act between employees.*

*Aubrey: Mhm*

*PS1: I guess is what I'm saying.*

*Tom: Yeah.*

*PS1: Once you log in if you wanna keep logged in all day, that's fine.*

*Aubrey: Yeah, I guess if everybody has the same access*

*PS1: They do! Everybody has the same access, so it really doesn't matter as lots of times you don't really have to be using the computer that you are logged into. You can go and use somebody else's login or you know.*

*Aubrey: Mhm.*

*PS1: If Becky's logged in over here and you need this computer you can go ahead and do it.*

*Aubrey: Mhm. Does your*

*PS1: because its the same information.*

### **9.63 (Temporarily) Missing Child (Study 1)**

Observed:

- Child-P01 2009-10-13 3:40PM – 4:50PM
- Child-P01 2009-10-13 5:25PM – 5:30PM
- Child-P01 2009-10-14 11:15AM
- Child-P01 2009-10-14 11:20AM
- Child-P06 2009-10-23 3:15PM

Interview:

- Child-P01

There were actually a larger number of incidents of directors being unsure of the locations of the children in their center than I would have suspected. All of the incidents that were observed were centered on the transition from the bus to the childcare center. This transition is difficult to coordinate because of the number of local variations. For instance, if the bus driver is sick then there can be a bus driver who is unfamiliar with which children are supposed to be co-located; parents can pick up their child that day for a special event; and, children can be sick and parents can forget to let the childcare know. These local variations lead to difficulties in tracking where children are and can result in children being temporarily missing.

The largest incident that was observed involved Child-P01 when Stacy was observing a director at a childcare center that had only been open a couple of months. Stacy's notes are fairly comprehensive and included below. The summary is that PT7, who is a teacher at the sister childcare, her child is temporarily missing. The incident starts when PT3, the assistant director who handles staff files, enters PT1's office while we are interviewing her asking for the PT7's cell phone number – presumably to call her and ask if she knows where <child> is located. PT3 tells PT1 that the teacher does not know where <child> is located. The incident continues to unfold until the child shows up with PT7 at the center without either knowing that the center could not contact any of them and as far as the center was concerned child was missing.

This breakdown involves directors, the bus driver, the teacher, mom and dad, the other center's administrators, and a whole set of places where information is stored about the child. The first breakdown is because the center did not have updated information for PT7 or her husband. The second breakdown is that when they did find a number that was correct for the mum from the other center the mother did not pick up her phone. The third breakdown is that the bus driver was not able to know whether or not she was supposed to pick up the child that day after school. The fourth breakdown is that assistant director from Child-P01 was waiting for information to be updated from the other sister childcare.

The other instances demonstrate cases where parents forgot to call in a child, where parents were unsure where their child is currently located, when a parent calls in late that their child is with them, when a child tries to not get off the bus and instead tries to go home instead of the childcare center, and a case where a child who did not attend the childcare got off the bus.

The director from Child-P01 tries to explain her policy on the transition from childcare to bus:

*(2009-10-14 11:15) "So, we just uniformly write it there, they check it before they leave. If the vans have left and a phone call comes in, then we're calling them on their cell phone, 'hey, Joey's parents just called, he is not riding the van today' so that they have that there... well, it's lots of little lives, you know I tell people all the time with the track down policy-- we charge them \$5 every day that we have to call them to track down their child. We bill it to tuition to make it a true payable thing, it's not a courtesy. But, what's scarier, the parent losing the child, or the teacher losing the child? I was like, you can sue us... you can be mad at yourself, but you can sue us, and that's just not a risk we're willing to take. It's a very scary feeling when they're not coming off the bus."*

All of these incidents indicate a place where the lack of adequate documentation results in inadequate control over a child. Not having knowledge of who should be on the bus each day is going to result in missing children. In activity theory this breakdown results due to inadequate tool support, but also when activities have obscured outcomes. For instance, it is not clear to parents that having their information, like phone numbers, updated can result in the childcare not being able to contact them if and when their child

is missing. The perceived infrequency of this event also does not induce childcares to update their information in the bus as quickly as they should.

Design Implication:

- Support sending notifications of missing children from the bus
- Support distributing updated information across numerous information systems in real time

Child-P01 Observation Notes:

*2009-10-13 3:40PM Yet another figure appears in PT1's door, the assistant director PT3 (InterviewP1Oct13.mp3, [00:37:44.13]):*

*"excuse me, do you have the cell phone number for PT7?"*

*"I do not..."*

*"darn"*

*"why would you need--"*

*"PT8 not sure about <child> 'cause she's not there, but today's she's supposed to pick her up."*

*"uhh, you could probably call over to <sister center> and see if they have it"*

*"Yeah that's a good idea"*

*"they still might have it"*

*3rd person (PT8?): "I don't have it here"*

*The parties exit and we continue the interview.*

*4:10PM Another figure appears in the doorway and kicks off an extension a thread started during our interview. [It appears that there has been a critical incident with respect to lack of information; I can partially tell by the tone of the speakers, the tension in their voices and the dancing around topics that takes place]*

*(ObservationP1Oct13.mp3,[00:04:44.16]):*

*"Did PT7 mention that <child> is not going to come in on Tuesdays?"*

*"She didn't say anything to me"*

*"I left her a message to call me, but both <child> and her classroom teacher says that she wasn't coming today."*

*"Ok, did you call PT9?"*

*"No, I haven't, I didn't have her number in the van yet, so I got her mom's number." [said hastily, in a defensive way, as if she knows that she is in trouble]*

*"You've got to get those numbers in there" [said with soft voice, serious tone]*

*"I know, actually what I was going to do--I talked to you about it--is, tomorrow morning, can I take my laptop back over to the other site to update theirs. PT4 is just--"*

*"Sometimes what I do, though, is I just made a separate sheet I didn't even plug them in. I just said "phrumph!" here are all the numbers, you know."*

*"Ok"*

"So, I mean, you don't necessarily need to update in their--well, I guess you still have to go to get the numbers, though."

"yeah"

...

"no. I sent her what I had and she said she was having every time she'd do it and then try to save it, it'd disappear and she was just not at it. So, I just was like 'no', I just need it done, so I'm just gonna take my laptop over there and do it <laugh>. Cause that's what I've been waiting on, is her sites. Um, yeah so I'll call Scott now. I just, you know the teacher said that she had a conference with mom this morning, and that mom said that she wasn't doing it anymore on Tuesdays. So, I left PT7 a message, but that was the only number I had with me."

"Well, I mean PT7 did go home for the day so I mean that's a safeguard that she's not coming, you know, so I'd say that's highly unlikely, but. We don't have the ring \_\_\_ over here?"

"we don't"

"M\*\*\*, PT7, and <child>'s?"

"I think they are, I just, I only have mom's with me on the bus."

"Ok, cause her cell phone should be on it"

"That's what I called, was mom's cell phone, cause that's just all I got. I asked PT3 for it when I called I\*\*"

"ok"

"I'm surprised I couldn't reach her on her cell, but I'm just looking for the green card right now to follow it up. I had to track down two staff kids today 'cause J\*\*\*\* forgot to tell us."

[I can't make out exactly what's happening here. The confusion this dialogue calls makes me realize just how much contextual knowledge the two ladies are using to make sense of their own conversation; the story is not complete with these words only. Together with the dialog from 3:40, it seems that <child> is a student that usually does not ride the bus home on Tuesdays. But, second-hand knowledge of a parent-teacher conference earlier that morning led her to believe that <child> would begin riding the Child-P01 bus home on Tuesdays. When the bus went to pick her up today, she was not at the stop. The bus driver used the contact list on board to call PT7's cell phone (potentially both a teacher and <child>'s mom). PT7 could not be reached, so the bus driver seems to have called I\*\*. At least 8 people (PT7/mom?, <child>, I\*\*, PT4, PT3, PT9, <child>'s teacher, J\*\*\*\*) are involved in this situation, not including PT1 and PT8 (perhaps PT8 is the discussant in this 4:10 conversation?) from the 3:40 conversation. The fact that so many people are intertwined with one event makes me think about the community effort that goes into running this business, raising these children. And, it shows how distributed the information and responsibility can be.]

...

"But, back to the phone numbers," PT1 began (ObservationP1Oct13.mp3, [00:10:55.07]) after B\*\*\*\* and family headed off to visit with her friend.

*"They did not have all the phone numbers completed"  
"in the car? so that they couldn't call somebody?"  
"normally what happens is that they call here and we give them the numbers"  
"and, did that happen earlier?"  
"it did not happen with me, so it might have gone to PT3, I'm not 100%...  
but I will get to find out later, because PH1tine's gone for the day"*

...

*4:50PM This phone call is yet another in connection with the phone number complication that happened earlier in the day. It went like this:  
"Good afternoon, Child-P01, this is PT1, how may I help you?"  
"PT7-to-pea-to!?" <sounds like this is someone's nickname, PT7's, I presume>  
"Niiiiiice, PT7. I told her "darn, she's left the building, they're not coming."  
[The teacher (PT8?) from the 4:10 discussion must be who PT1 is referring to here. It also seems that PT7 is <child>'s mom, and also a teacher at Child-P01 (confirmed on their webpage). Since PT7 had gone home, it was unlikely that the Child-P01 bus was actually supposed to pick <child> up. But, because policy requires the bust to stay until contact is made, the bus had to wait. The bus driver (Pt8?) called I\*\*, who then contacted PT3 in order to get PT7's cell phone number, but she couldn't be reached. There is no clue as to when or why the bus actually ended up leaving the site (e.g., did it leave before getting confirmation form PT7?) It seems as if the home phone number was missing from the bus binder. Also, perhaps PT9 from the 4:10 conversation is <child>'s father? I google for 'PT7 Rainbow Riders' online and find that PT7 is a teacher (<http://tinyurl.com/ybgyvqm>) and PT7 is the president of the PTA (<http://tinyurl.com/yevzho3>). I google for 'PT7' and find that PT7 & PT9 are VT alum and had a baby girl in 2004 (<http://tinyurl.com/yf8evv8>)—putting the girl in the 5 year old range, a bus rider for kindergarten.]  
"Ok, so for both girls?"  
"Ok, I will let her know"  
<laughing>  
"I know, that's why we have the policy we will not leave the school"  
"Because, I mean they really--it's a little scary...like 'oh, I think they're gone', and I was telling somebody today 'sometimes we say 'oh yes, they are a car rider' and then 'oh, they were in the bathroom' you know?"  
"But still, I was like, just make sure..."  
"Ok"  
"I will, alright, bye"  
PT1 hands up and immediately makes another call using the internal intercom system into Laura's classroom: "Hey Pt8, that was PT7, they're not doing Tuesdays, they're only doing early releases."*

2009-10-13 5:25PM then the phone rings-- "hold on a second"  
(ObservationP1Oct13.mp3, [01:22:50.27]):

"hey M\*\*\*\*\*" "I thought he was gone, I'll see if I can find him, but I can't guarantee"

"OK, well, I'll try to grab him"

I'm confused when PT1 doesn't take any action to find "him" after hanging up the phone--no phone call to a room, no walking about the building or asking around. In the mean time, PT1 says "bye" to yet another exiting child (ObservationP1Oct13.mp3, [01:23:42.02]).

There's another ring and PT1 picks up (ObservationP1Oct13.mp3, [01:24:27.12]):

"hey, she did, she got picked up—B\*\*\*\*, right?--Basil was picked up about 15, 20 minutes ago."

"she was really sparkly, eating pumpkin seeds"

"you're welcome, byebye"

5:30PM I am tickled to hear this conversation; it seems as though a parent was actually unsure as to whether her own daughter had been picked up. I try to confirm that this was, indeed, a parent by asking PT1 (ObservationP1Oct13.mp3, [01:25:05.01]): "so, parents sometimes call to see if their kid's been picked up?" She responds with, "yeah, sometimes they are just a little unsure who's supposed to pick up, and sometimes they worry that their spouses forgot, if they're not used to picking up."

2009-10-14 11:15AM "like, I already have it in with the bus drivers, I hate that, you know we're sitting down with our list and we're crossing off, and they see the last child get off and they pull off and I'm like, 'I need to check for everyone'. We've had children miss the bus stop before, we've had to call the school and call the bus and be like 'are they on there?' 'yup they are, loop back around and...' We had one year where we had a fellow kindergardener not from Rainbow Riders to get off at the bus stop. And I remember doing the list and I was like, 'I have one more' and I look down and go 'honey, who are you?' and he told me his name I was like 'and, why are you here?' 'because they told me to get off' 'who told you?' 'she did, she wants to play.' So, I had to call the school, I'm like 'I know you can't give out the number, but I've got this sweet little boy here sittin in my office dropped off' and I kinda wish that, you know, the school busses had to follow the same policy."

2009-10-14 11:20AM "there's only so much you can do, exactly, and it's scary because you have to act fast because if they're on the bus heading home, you know we had one little girl for weeks on end we would be like standing up at the door and the bus would pull of and we had to put our hand on the door and be like, 'wait, she has not gotten off yet,' because it was the same bus that dropped off at our school but also dropped off at her house, and she chose to skip Rainbow Riders and would stay on on purpose, and so her mother and I were battling it, but if we didn't catch it,

*you know, she was on her way home to an empty house, you know sitting down at the doorstep, what do you do? Thank God her mom worked next door: 'come noooow! she did it again, she did it again, go get her, go get her.' So, yeah, it's quite a little thing."*

Child-P06 Observation Notes:

*2009-10-23 3:15PM There is no daily checklist for listing who was present/absent that morning. I asked PE1 about how they keep track of which kids to pick up, how they know if someone was absent any day. From her answer it seemed to me that those who drop them off know whom to pick up. Later when PE1 was helping the children get buckled up I heard her asking one child about another child, whether the other child came to school that day or not. My feeling, they rely on their memory. Since the number of student per van is small, I guess they don't want to go into the trouble of checking the list every day.*

Child-P01 Interview Transcript:

*PT1: we call parents if their child has not shown up for the day and we do not know why... you know typically by like 9:30, we just want to make sure things are okay*

### **9.64 (Temporarily) Missing Child (Study 2)**

Observed:

- Child-P01 2010-08-31 3:35PM

There was only one instance where there was a temporarily missing child in Study 2. In this case PT2 has picked up the phone with a phone call from a parent. The parent has waited until the last minute to call and say that the child will not be on the bus that day. PT2 tells the parent that normally the bus would have left already. At this point the child would have been marked as missing and effort would have been made to track down the child.

In this breakdown, as in the ones found in Study 1, the breakdown is a result of the parent not prioritizing the activity of the childcare accounting for the child. The parent is engaging in their activity of taking the child on a special outing, and neglects the activity of notifying the childcare.

Design Implications:

- Support lighter-weight mechanisms for parents reporting that children will not be present.

Child-P01 Observation Notes:

*2010-08-31 3:35PM PT2 grabs her pink sheets. She says that <childname> isn't on there. She says that it is a good thing that the bus hasn't come yet. I think this must be a mother, because PT2 tells her to*

*give a man a hard time. This must be mum calling in a child not going to be picked up on the bus at school.*

### **9.65 Difficulties Gathering Information from Parents/Staying Up to Date on New Information (Study 1)**

Observed:

- Child-P01 2009-10-13 4:25PM
- Child-P01 2009-10-13 5:15PM

Interview:

- Child-P01
- Child-P03
- Child-P04

The inability for the childcares to gather timely information from parents was a repeated pain point for childcare directors. The director from Child-P03 explained that parents come in, want to grab their child quickly, and then leave. With so little time for the parents to spend with their child every day parents are quick to leave the childcare center. Parents were reported to not value returning forms and providing information about their children.

To deal with this problem the childcare directors utilized numerous mechanisms to try and gather information from parents. For instance, PP1 from Child-P03 prints out a list of all the children and uses it to check-off when she knows a parent has returned the new information. For the parents who still have not turned in their papers she will then start to call them daily to hassle them. Child-P01 has numerous “READ ME” posters in the environment to get parents to sign-up or be aware of events/information in the environment.

This breakdown results in competing activities. Parents do not prioritize the activity of updating their child’s file, and thus the activity is not completed. In Activity Theory terminology, the objective of the activity is not clear to the parents.

Design Implications:

- Support automatic notifications to parents for when their child’s information needs to be updated.
- Remove the information in the environment and present one direct information stream for parents to attend to.

Child-P01 Observation Notes:

*2009-10-13 4:25PM PT1 tells me more about the immunization check-off lists when I ask (ObservationP1Oct13.mp3, [00:20:54.15]):  
"so, what sort of work are you doing with the immunizations?"  
"Immunizations actually back-pedaled--five seconds after walking downstairs 'ooh, I have to finish off those cross off lists for the classrooms', but the immunizations what I do traditionally what I do, once I have everyone near updated, I have this notebook that I use, the user*

*friendly contract part, where I can write down the child's name, do they have all their forms? Physical immunizations I further blow out--this is where technology would come in much more useful--and then I can keep track of their shot series they had, make notes of when the next one's gonna be due, so that every month I can just flip through and just say 'yup, Johnny, next set coming around, I'll send out a reminder note' "do you have to do that, or is it just something you do?" "well, the parents don't always give us the information <hands me paper, (Figure 5)> what I'm missing still, or what I need an update on" "you have to do that just once a year or is it more often?" "well, depends on the age of the child. A lot of immunizations are done by the time they are 18 months and then they are good until kindergarten, so those that are infants and toddlers, I'll check pretty much once a month, and then those going off into Kindergarten are checked the summer before they go to kindergarten." But, there are other things, like sometimes their emergency contacts are not local, so I have to make notes to myself that I haven't gotten it yet, make sure that I'm still hounding them for it--"*

*2010-10-13 5:15PM Finally, I take pictures at the entrance to the lobby, with the main entrance to my back. There's a poster board on display for all to see. In bright colors, with a large arrow and the text "Read Me!!!", there is no doubt that this poster is trying to grab the attention of parents. These arrows, coupled with the information posted on the classroom doors and on the main entrance interior doors, all seem to reveal a sense of struggle on the part of the daycare workers to effectively communicate with parents. These items are placed in highly-visible locations--at transitions between spaces where most parents must go (through the main entrance, through the lobby, to their child's classroom door).*

**Child-P01 Interview Transcript:**

*PT1: Sometimes, it's us calling saying 'you know I sent you two letters [something about immunizations] and I haven't gotten yet I really need to have it', you know, just calling in doing that verbal reminder to them there.*

**Child-P03 Interview Transcript:**

*P3: from the office, I do have email, we have a website and so my email address is PPI@Child-P03 so I do have parents that utilize that, they're on the computers all day - that works for a good chunk of parents, there are some parents that have not figured that out yet that we've got out there that we have a web address that we have email accounts... i have a lot of parents that just call but if i need them to have something definite then i give it to them in hand writing and in something on writing on paper... a lot of the times what i'll do is just do that from the front desk and just print out a roll sheet of the entire facility and then after we hand it out we check off that we've given it out to make sure that i know everyone - so you can't*

*come back later saying you didn't get one... but we try to do verbal and written and we try to remind them verbally and give them something because most of our parents actually had - i actually had to take apart my parent handbook and take the agreement sheet off of the back because i found out that most of the time i was getting enrollment forms i wasn't getting that sheet back because no one reads the handbook*

Child-P04 Interview Transcript:

*Interviewee: "Oh yeah, they'll say 'I didn't know there was a parent meeting, and we put out an annual calendar just like this that captures August 6, 2009 through August 4, 2010. And, they'll still say 'I didn't know there was a potluck tonight or--And, we do, the classrooms do monthly newsletters, too, so they always capture important dates there. But they're still 'I just had no idea.' So, yeah, that does happen here. I know in the blue room, they tried to get photographs, they wanted family colleges, and I think they finally got up to about 50% participation. That was after, you know, a face-to-face transition meeting, they gave them the form, you know 'we just want to make a collage, we want to get some family pictures up,' a couple newsletters you know reminding them, and then at the parent meeting they reminded them. And, they were like 'we don't know what else to do, PUI.' Well, just put up the ones we have. So, yeah, our parents are busy and juggling a lot, so it does, it does."*

### **9.66 Difficulties Gathering Information from Parents/Staying Up to Date on New Information (Study 2)**

Observed:

- Child-P01 2010-09-02 2:42PM
- Child-P04 2010-09-08 9:47AM
- Child-P04 2010-09-09 11:22AM
- Child-P06 2010-08-30 12:55PM

Childcares have difficulties gathering new information from parents. When a child is first enrolled they provide extensive amounts of information about their child in order to ensure enrollment. After the child has been enrolled, though, information about the child may change. The simplest example is that a child may receive immunizations and require a new immunization form to be provided to the childcare. Gathering this new information is difficult for the childcare because, as it is perceived from the childcare personnel, the parents are too busy and they do not value returning that information.

There are many mechanisms that have been utilized to try and gather the new information. For instance, I was able to observe a director for three hours while she was going through all of the children's files to see what information was not up-to-date. The mechanisms she used was texting parents for information to their cell phones, sending the parents emails, and also putting copies of the papers that need to be updated on the outside of the file for when parents come by.

There are numerous cases where the information that the parents have provided is not up to date that were observed, and this was a main pain point for the childcares in terms of managing the child's information. This is important for licensing, but also for contacting parents during emergencies. This breakdown occurs because even though there is an explicit rule stating that parents need to provide this information, the objective of this activity is obscured. Parents do not value nor do they understand this activity, therefore they do not provide the information.

A second issue related to this problem is that childcares are inundated with information. Everywhere you look in a childcare there are poster and papers on the wall that need attending. For instance, in Child-P06 when you enter there are flyers for computer classes, papers about notifications such as being closed on a certain day or class pictures. These are displayed before you even enter the center. Once you enter the center then there are copies of health inspections, DSS inspections, and occupancy restrictions. Pictures of the entryway boards are included below.

How inundated parents are with information exacerbates their ability to attend to what is salient. Each of these information boards has a conflicting objective and duals for the attention of the parents. In a way, this problem is a recursive: because the childcare personnel have problems communicating with parents more information is displayed in the environment; because there is so much information present in the childcare center's environment parents ignore it. For example, during all hours of observation parents were not observed once to read the bulletin boards that are carefully constructed for them.

#### Design Implications:

- Support automatic pinging of parents to get new information.
- Provide a method to let parents know that their information may not be up to date, and the consequences of this.

#### Child-P01 Observation Notes:

*2010-09-02 2:42PM I follow PT2 back into her office and PT4 comes in as well. PT6 tells PT2 that there is a student, remember how PT2 sent a packet of information to be filled out. PT6 says that they've been bugging the parents about this information since we was in the baby room. PT2 asks what they are missing. PT6 goes to get his file. PT6 says that they haven't gotten an updated form since the child was 4 months. PT6 lists of all the reminders they've sent to the family, with no response. PT2 says that she'll bug the dad when he comes in today.*

#### Child-P04 Observation Notes:

*2010-09-08 9:47AM She then paper clips the paper to another set of paper she has, and put the on the desk. I ask if those are papers for parents to fill out, and she confirms saying that these are papers that parents 'didn't do'. She puts the folder she took out onto her bookshelf and opens another folder, types in a child's name onto her spreadsheet, and starts to tab through the folder.*

*2010-09-09 11:22AM Since it is the start of a new school year each student has to turn in a new registration form, a permission slip, and a health form. So she is going through those as well as she goes through the children's files. She says that lots of the time the parents don't fill in the forms correctly.*

Child-P06 Observation Notes:

*2010-08-30 12:55 PE1 explains about the problem with communicating with the parents as a 'never ending battle'. A girl comes and punches her timecard to checkout. PE1 says that she has a problem with getting the parents to communicate with them accordingly. They've tried newsletters, both electronic and physical. But the problem is that parents don't want to read them. So they've tried putting the information out for when the parents come in. The current problem is that parents read the re-registration fee, and paid that, but didn't pay the supply fee. She she's going to have to go and show them the form again to get the payment.*

### **9.67 Client Files Dispersed in Environment (Study 1)**

Observed:

- Child-P01 2009-10-14 10:30AM
- Child-P01 2009-10-13 5:05PM
- Child-P03 2009-10-21 10:17AM

Interview:

- Child-P01
- Child-P03
- Child-P04
- Child-P08 (2 instances)

As we discovered in our observations, information about the children in childcare centers is dispersed in the environment. There was primary information that was stored about the child in a central file that the licensor would require, but then information was also in many other forms in the environment. For instance, we saw files in an electronic form and in paper form. We saw paper files for the official information, separate files for accident reports, and another one for documenting sensitive information. We also saw that there were files kept about the children in each of the rooms that the children spent their days in. Child-P01 and Child-P04 also kept books documenting a child's developmental progress that were shared with parents. Apart from large chunks of information, there was also information about the children in their families in family directories, rolodexes, in running journals of what was going on in the center or each room, in daily write-ups of activities in the room, on display boards, on sheets for dietary concerns, post-it notes with names and contact information. The ubiquitous distribution of client information in childcares was salient.

Specific examples of how information was distributed in the environment and the reasons for distributing information are included in the interview transcripts and observation notes

below. For example, PT1 from Child-P01 discussed how when she was first starting to run her center child files were all over her office because she “needed” to have them out to get to everything. Similarly, PD1, who is the licensor for many of the childcares in our study discussed how certain information about the children need to be locked up. But, she also recognizes that to be able to properly care for children information has to be displayed in the environment for the teachers. At a basic level this is allergy information that can help save a child’s life. However, much more information is in the environment than just basic information.

The breakdown occurs here because there is a false sense of security. When parents ask where their child’s information is stored they are shown a locked filing cabinet that only a few people can supposedly access. This creates a false pretense about how distributed the information actually is. If parents were aware of the number and location of all of the places that their child’s name is located, let alone information such as their address and phone number, they would be shocked. This is not to necessarily say that the childcare centers are not keeping the information secure. It is merely to note that there is ambiguity surrounding how information is being managed.

#### Design Implications:

- If it were possible to know all the locations of a child’s personal sensitive information, do not necessarily share this information with parents – perhaps create a meta-construct that displays locations of sensitive information but not the density.

#### Child-P01 Observation Notes:

*2009-10-14 10:30AM PD1 turns to me and asks "do you have any questions you want to ask me while I'm here." I'm almost too excited that she's asked me this and I fumble my words at first (ObservationP1Oct14.mp3, [00:57:54.22]):*

*"like, things in the filing cabinet, is that any matter, behind a locked door, or things like that?"*

*"things have to be kept confidential and locked, per se, but the staff still need to be able to have access to it even if she's not here and for emergency contact information. So, sometimes they will produce their own emergency contact form for their classroom--"*

*PT1: "that's what the green cards are--"*

*"--yeah, and that way this can remain locked but people still have access to the information needed"*

#### Child-P01 Interview Transcript:

*PT1: We had a mass enrollment of about 200 children, so I was processing paperwork and I had piles on my floor. And, so when the kids were coming in, I was like 'oh my gosh, I have to move these piles' and the same for the woman across the way for me here, she had staff files and so, trying to keep the children out of it, but at the same time, we still needed to have them out, so. Keeping organization skills down has been a big issue.*

Child-P03 Interview Transcript:

*PPI: We do have to access the file. Umm, if there's an accident, bites, things like that, umm they may need it for medicine. Umm, we have to make phone calls. Amm, we print out information sheets for the teachers that have what was that in our system, that has a, just a compacted list of child's information sheet as the parent's work information, home information, phone numbers, pick-up people. So, the teachers have a folder accessible to them in the room.*

*Laurian: how do teachers get access to the child's file?*

*P3: they don't... i give them that information on the information sheet, what's in their file that they need to know is their allergies, their chronic physical problems, any kind of therapies they're given, any kind of medications they're allergic to... all of that prints up in a report... [shows ProCare report on laptop]... so i have a child that has religious reasons why they don't eat certain things and has some developmental delays... so that's in her file in the notes and comments of child tracking but when I print this report for the teachers it's a specific report, it's an information sheet and ... it has the parent's information on there and so if they need them for anything they have their contact information and here it will list under someone's name, her date, her classroom, you know, her gender, and it tells about her developmental delays and um==*

Child-P04 Interview Transcript:

*Interviewee: "If--one instance, we had a child who was injured onetime, and so whenever we call the rescue squad then there's their enrollment form that has a lot of pertinent information on it. What we've done, um--because the last one actually happened when I was at the doctor's myself (which is kind of ironic)--so they were able to get to the file, but what happened is, then they needed to make a copy, which took away crucial time. So, what the rescue squad folks recommended is that we make a copy of that form for every current child and now we keep that in a folder, and that's in a file room. So, that if it happens again, we can just open the file, 'here's the sheet' and they can take it with them"*

*Stacy: "And, that's in this file?"*

*Interviewee: "The actual file we keep in the file room, and it's actually with our first aid kit, and it's just their enrollment sheet. And there are some things--it's hard, because some information is treated as confidential, but some of it has to be very accessible. So, um, you know we have emergency contacts so if we have a fire drill or a real fire or any other reason that we need to evacuate, we need a quick way--and you know it would take precious time to pull those files. So, on my door, there is a blue folder that says 'emergency contact information', but we also put the word 'confidential' on it. And, that is kept on my door and it has the children's name, the date of birth, their parents' name, and their address*

*and phone numbers for their parents and emails for their parents. And they're, you know, I could keep them locked up, but if there's an emergency... So, we've found that by putting 'confidential' on there--we've never had a problem. And, quite honestly, the parents have asked for classroom directories that has most, if not all of that information anyway. But, then they sign--you know, as part of the form, what part of that they want included in the class directory. You know, we explain that this is something that you guys will share among yourselves to plan birthday parties, play dates, things of that nature. Most of them--it's the same information--and then there's a few who just want their email. So, for that reason I try to be mindful of that information being on my door."*

Child-P08 Interview Transcript:

*Tom: so do the teachers get access to the children's files freely?*

*P8: they have to come through us (the director and admin assistant)... they get - we have a one form that parents fill out that is supposed to be in the room with the child at all times because it's their emergency contact information and their medical release*

*Tom: yeah, and that's all stored in the room...*

*P8: that's stored in the room, yes.*

*P8: teachers have just the student info sheet, they can access incident and accident forms, they keep a log of incidents and accident - like they turn in the sheets but they keep a log of what child did what to whom*

*Tom: so where is that log usually stored?*

*P8: they have a notebook in the classroom and that's where they keep the child info sheets and that log, like a behavior log they call it*

Child-P01 Observation Notes:

*2009-10-13 5:05PM I make my first stop at the Blue and Aqua rooms, which are immediately to the right as you head down the "long hall" that's across the lobby from the kitchen. The doors are side-by side, with a bulletin board and desk sandwiched in between (Figure 6). The doors, wall, and desk are littered with information--papers, binders, file folders for each child, and whiteboards. There are informational sheets, sign-up sheets, lists with the names of children, the teacher's name, names of substitutes, classroom illnesses, birth dates, artwork, daily activities, and more... The types information that I thought might be considered more private are exemplified in Figure 9. On the left, there are three instances of daily activity logs, which sometimes contain the names of children and things they did that day. On the right, there's a pin-up of the a daily schedule that identifies who opens and who closes, and when other significant activities take place throughout the day. In the middle, there's a picture of a binder and a file stand that seem to contain information pertinent to each child. [I suppose the binder has old copies of the daily summaries we see in the leftmost picture in Figure 9, while the file folder*

*may be what PT1 is talking about when she discusses the tax forms]. Regardless of what is in these last two, I feel afraid to look into them. There's something about the binder that makes it seem less public, even if it is out on a relatively unguarded desktop. I'd have to take it out and open it to look at it--a more visible action that might require me to explain to a passerby what I'm doing. The files, too, give me this impression. Actually, the files seem even more off-limits to me. I tend to keep personal information in my own files, so I already consider files to be for somewhat private information. The fact that there's a child's name on each tab makes an even bolder claim to their ownership--and my lack of ownership--of the information in the files. I want to know what type of information is in these places, but I decide not to look for these reasons].*

Child-P03 Observation Notes:

*2009-10-21 10:17AM The classrooms have a big notice board with the meal plan and weekly activity information. Beside the entry door, there is a telephone mounted on the wall. All over the wall, there are lots of forms. Most of them are printed and are related to emergency number, emergency procedure, emergency exit plan and route, playground schedule, instructions on how to cough. Allergy information is handwritten and clearly visible. [The picture below shows] information behind the door. (The allergy information is covered).*

### **9.68 Parental Over Restriction of Access (Study 1)**

Interview:

- Child-P01
- Child-P04

Both Child-P01 and Child-P04 have a form that parent's fill out forms saying who can access what information about their child that will be displayed in the environment and stored in the child's form. An example from Child-P01 is included below. If a parent agrees that it is ok for certain people and for certain information to be displayed then the parent would initial the box.

In the quotations below PT1 from Child-P01 and PU1 from Child-P04 both talk about how they would try to respect the parents wishes. So if the parent said that they only wanted the director to be able to see the information, then they would try to respect that. There are times though, when certain information is necessary to display in the environment just for the safety of the child. Examples include allergies and emergency contact information, which the directors want to be present in the kitchen and in the classrooms.

To deal with situations where parents have overly restricted who can access their child's information the directors say that they will then discuss case-by-case issues to negotiate who can access the information. This breakdown illustrates a case where explicit rules for managing the information are not actually that hard and fast rules. The actual rules are

that parents are allowed to try and restrict access, but if the childcare thinks that they need to display that information, they will.

Design Implications:

- Keep track of places where access has changed to highlight places where there is less room for negotiation for confidentiality.

Child-P01 Interview Transcript:

*Laurian: "And if the parents say 'no', what would you guys do?"*

*PTI: "Then, we can't give it to them. But, sometimes they don't fill out the form correctly, so I go up to them like 'k, so you're saying the director can't look at that, that means I can't prove your paperwork, can you please you know understand that my role is this, you know to make sure your child has everything they need to be in our school, that they've received immunization, they are who they are, da-da-da-da, I'm not giving it out,' then they're OK with it. Montgomery County Public Schools, Early Intervention, yeah, we're not going to push it; that's their parent right. If we do have a concern about a child's development, though, and we really think there's something going on, we'll still have a conference with the parents to say, you know 'it's out of our realm of experience, we're seeing things, we need more tips and suggestions, please would you consider having this person come in as a third party, unbiased observer of your child to see what strategies we can help them prepare themselves for kindergarten.' And, normally they are pretty responsive to that."*

Child-P04 Interview Transcript:

*Stacy: "Are there any--if a parent didn't agree to let a teacher see a certain type of information, would it be a situation where they wouldn't be able to have their children stay here in the daycare, like say the emergency contact information, if they didn't allow a teacher to see that, would that be--"*

*Interviewee: "yeah, that would be a licensing issue, because that's a health and safety issue. So, yeah, that would"*

*Stacy: "But, could you name something that wouldn't be a licensing issue"*

*Interviewee: "Like, those background forms that I talked about, where they write about just the child's development. I can tell you what it's called. A lot of the stuff that's in the file the teachers have actually completed themselves. It's just an enrollment question here. There is a physical and immunization form in here that teachers really--like that's something that I would need to see, just to make sure the child is cleared to be in here, so a teacher wouldn't necessarily need to see that. That enrollment form that's probably where I would have to say, you know, the teacher's need that information because it includes, you know, the emergency contacts, allergies that the child might have--those are some crucial pieces that the teachers have to know. The allergy information we even have posted in the classrooms, but they sign permission forms"*

*allowing us to do that--to display it--otherwise we would have had to use a folder like this and make sure that all of our substitutes know where the folder is, and I think with an allergy the parents are usually totally in agreement. Yeah, put some neon lights around it "*

### **9.69 Securing Children (Study 1)**

Observed:

- Child-P01 2009-10-13 4:20PM
- Child-P01 2009-10-13 4:35PM

Interview:

- Child-P04
- Child-P06
- Parent-P11
- Parent-P12
- Parent-P18

The reason I decided to include this theme is because I think that the management of the child's care and management of the child's information are deeply entwined. Thus, to really understand breakdowns in managing sensitive information, I should also include breakdowns relating to the security of the children.

In two examples below from Child-P01, PT1, who is the director, talks about the new key fob system that has been installed in her center. This fob system is set a little above waist level, if I remember correctly, and parents have to wave their personalized fob across this box and then the doors will open. The problem is that sometimes parents would not know where to wave their key fobs, or if their key fobs were successfully waved. This leads to parents having to be buzzed in. The problem with buzzing in is that it relies on someone recognizing the parent or someone asking the person who has entered what they are here for – functioning as a sentinel. As demonstrated in the second example from Child-P01, PT1 lets in a mom because she looks like she “belongs here.”

The breakdown occurs because the key fob system still requires the social system as a fall back when the electronic system does not work correctly. The social system cannot correctly identify 200+ parents to make sure that they should not be in the center. This allows for a security breach in the physical protection of the children in the center.

In another example PU1 from Child-P04 talks about how there was a policy change after a fieldtrip. A child came back from a fieldtrip and talked about how she was happy because she did not have to ride in a car seat. With a little investigation PU1 discovered that the parent who drove the child to the destination was not aware of putting all children in car seats. The new policy is now to check that all children are buckled in car seats before leaving. In this case the breakdown happened because the implicit rule to put children in car seats needed to be made explicit.

The last example comes from PE1 from Child-P06 explaining an incident from the childcare she previously worked within. There was a parent with a custody issue who

came into her center and made threatening remarks to be able to access his child. This breakdown occurred because a parent was breaking the rules outlined by the government.

Child-P01 Observation Notes:

*2009-10-13 4:20PM I asked her about the arrows taped on the breezeway wall, pointing at the doorbell and the keyfob swipe (ObservationP1Oct13.mp3, [00:15:03.22]): "We didn't have our security system up, we were having some technical problems at first, and then there was problems with me getting data entered in time, so we told them that once 2/3 of the keyfobs were sold to the families, we would start locking doors because we didn't want to have to ring the doorbell three hundred times in the morning and three hundred times in the afternoon. So, those went up to inform them what to do. It's actually quite humorous, because when they got their fobs, I'd show them where the sensor was and showed them how to do it, and they would still come in and they were just looking around and looking at the ceiling... 'it's not on the ceiling!'... we try to make it user friendly, and it's particularly hard for families that have English as their second language. You try to say things as concisely as possible without disrespecting them. But, sometimes linguistically things just don't translate."*

*2009-10-13 4:35PM I'm surprised that PT1 didn't recognize the mother's face, given that she has been so ready to find the right name for all those parents and children coming and going, the people on the other end of the phone line--even parents and children on the waiting list. Later, PT1 confesses (ObservationP1Oct13.mp3, [00:37:08.18]): "it's hard because I get people's faces, but I still forget, like I'm like 'oh, it looks like she belongs here.'"*

*"Oh, sorry, I didn't recognize you"*

*"Should I get a key, or?"*

Child-P04 Interview Transcript:

*Interviewee: "And, this has been a couple years ago. But, we had a parent who offered to take another child and that child came back--wow, it feels really quiet in here --that child came back and he said 'I didn't have to ride in a car seat' we're like 'you had a car seat' 'but I didn't have to ride in it.' So, that was one instance where we sort of assumed--we did a car seat check, but did we take it the next step to really--you know we sort of assumed parents knew to put them in car seats, but in this case it didn't happen. So, we did have to add another step"*

*Stacy: "Oh, so you did add another step so that they actually make sure they get strapped in before they leave?"*

*Interviewee: "Yeah, the teachers check in the car, so there you go!"*

Child-P06 Interview Transcript:

*P6: I can tell you - it wasn't here but from personal experience we did one where it had to do with custody... we comply with all court - any center that's licenses complies with what the court says like if they're a custody dispute.. in the absence of that the biological parents have the rights to access the child but sometimes the court says otherwise and we had an incident in a prior program that I worked at where we had a parent that was biologically the parent but legally had been asked to keep their distance... (Huntington et al.) came in and was pushing to get access to the child... was - I say threatening, loosely, the teachers but, while the teachers wouldn't release the child - we called the police and that was how it was handled... because it was very early in the morning and there weren't a lot of staff in the building and I think that they felt really threatened - that may not had been his intent but that was how it was received.. so we would operate the same way here, if we had someone approaching in an intimidating manner I would not hesitate whatsoever to call the police and I would tell the staff the same thing... most instances where you come in and kind of wonder why somebody is standing around we would just approach them and ask them - because if it's a parent and they're in here they may be looking for somebody, an administrator - but because we are responsible for a large group of kids I don't hesitate to call the police*

Parent-P11 Interview Transcript:

*Participant11: The main reason was the security of the day cares. <childcare> the doors unlocked and there often is not anyone in the lobby area. At Blacksburg daycare the doors are always locked and there is a little button to ring and buzz her in and I can be buzzed in at that point. So, it was mainly security.*

Parent-P12 Interview Transcript:

*Participant12: Okay. They have said it. And this is very interesting since we had an incident last week. That only those who I have listed as permission to have any access to <child's> information, can see it being those are the people can call and ask how his day is going, what they feed, those are the one who can pick him up, those are the one who can call and ask about him. However, that is not occurred in practice what so ever. I had, there was an accident on the way home, I drive here to West Virginia, I was not able to get the daycare in right time. I had to send my mom and my dad to pick him up. But my dad is not in the permission list. I tried to call them. No one answered the phone cause it was at the end of the day but they let my dad come in and get him anyway which is fine, because he is my dad, but I didn't like the I mean they were just going to let him come and take my kid... So, that was very very disappointing. But yes they have access to anybody to call right now and ask "Hey how is <child> doing?" "Oh he is great." You know they are. So...*

Parent-P18 Interview Transcript:

*Participant18: I guess the only other thing that I would say that I find interesting that I just heard about, thought it worth sharing since you are collecting data. Like I said one of the things that they had you fill you these forms on who can pick up your child when you can't pick up your child. And for me I always in my list like the ten people who I don't mind to picking up my child and of course anybody who is not in my yes list is in my no list. But there have been times in the past where we just sort of of the couch made an alternative decision like my kid and this kid over here are both in Ty Kwon Do after school together so my kid gonna ride with that kid's parents the \*type window\* and there is never any amendment of the records, there is never any conversation around okay is that parent is on your list and it gets for me. I have an intact family. I am not protecting my son from anybody. There were not any major concerns around it. Then I think about, what about the mom who is in the process of his divorcing, her child's father abuse her and she is afraid that that child's father is going to take off the child violating custody or something like that. I always wonder like are the people at that building are really aware who the child can and cannot leave with, if they are really paying attention to that record, if I just said oh you know today my kids gonna ride with that buddy of the \*"type window"\* with that buddy's dad and if it were all casual how we know that the people in the building are really able to hold to the letter of the parents stuffs that they gave. I do wonder about that because some of the information are pretty high at step, I mean that is pretty important that if they are specific people who are not what picking up your child, do they daycare workers automatically know how to enforce that. That's just one thing I wondered about. It does not impact me but I am sure that...*

**9.70 Staff Accessing Client Information that they Should Not Access (Study 1)**

Observed:

- Child-P01 2009-10-13 5:00PM

Every childcare that was interviewed explained that everyone in the center was not allowed to have free access to a child's information that was stored. Specifically, the information that was stored within a child's folder in the director's office was to be managed by the childcare directors or administrative staff and teachers were not to freely access that information. The procedure, as explained to us, was that if a teacher wanted a piece of information, the purpose of accessing that information was assessed by the director, and if deemed appropriate the director would pull that information for them.

As shown in the example below, a teacher comes into PT1's office at Child-P01. She wants to get all of the middle names of all of the children in her classroom for a project. She walks over to the filing cabinet, and asks if she can "dig". This question implies that the teacher wants to troll through the files to extract the information, but that she seeks

permission from the director before doing so. What happens next is a negotiation where PT1 insists on the formal procedure, but what actually is happening shows that the formal procedure is not what is normally followed. This is not saying that social methods are not actually used, but merely that the formal practice of managing the child's information is not the actual practice, therefore demonstrating a breakdown from the explicit rules of process and the implicit rules of process.

This example is also important because Child-P01 has a policy where parents are able to restrict who has access to their child's information. Therefore, before being able to pass on any child information, PT1 would have had to check the form from the parents for each child before letting the teacher see the files. This is a formal breakdown between explicit and implicit rules but one that is not going to be remedied because parent's most likely have little knowledge that teachers can and do access their child's file without the director always being the go between.

Child-P01 Observation Notes:

*2009-10-13 5:00PM A teacher appears in the doorway and walks into the room and approaches the corner of PT1's desk (ObservationP1Oct13.mp3, [00:55:06.24]):*

*"Hey"*

*"If I want my kids' middle names, are they gonna be in here or in the file?"*

*<points to black box>*

*"they'd be in their file"*

*The teacher then says, in a much softer voice, "can I dig?" The informality of this word, the tone of her voice make this seem like a common practice. PT1 responds with a carefully-laid sentence and a slight sternness in her voice--her eyebrows raised, eyes widened, and a scolding manner in the slow, undulating movements of her head and voice as she speaks: "I'll have to dig for you." I can only see the side of the teacher's face, but she looks shocked in that her face pauses, gaze held with PT1's, and there's a space created that seems to beg of a verbal response. PT1 fills the silence with a soft, earnest "I'm sorry" that seems to answer the teacher's unspoken question: "I can't, really?" It convinces me that this is usually not the situation the teacher finds herself in. The teacher explains that she wants to make a name book with their full names and asks PT1 [as if to justify her request, perhaps to implicitly ask PT1 to reconsider] if she needs her to make a reminder note [as if to play with the notion that it's really just a small request and to suggest a heavyweight documentation of it in rebellion]. PT1 finishes with "I was gonna say, do you need them now or can I get back to you later?" [Perhaps PT1 is making space for the teacher to come back later to service her own request, when I'm not there]. The teacher responds meekly, an unexpected wrench put in her planned activity: "later's fine." The teacher exits, and then PT1 asks me to leave because the parent is coming her way.*

### ***9.71 Sensitive Information Displayed in Environment (Study 1)***

Observed:

- Child-P01 2009-10-13 5:05PM
- Child-P03 2009-10-21 10:17AM

Similar to what was discussed in the breakdown ‘Difficulties Gathering Information from Parents’, there is a large amount of information that is displayed in the environment. The effect that this has on the people who work there and the parents who pass through is that they are numbed to the sheer amount of it. As shown in the notes below, a description of the classroom day is displayed on the door to each room, there is a sign-in and out sheet, there is artwork, there is a tuition box with checks, there is a menu with daily alterations, there are daily log sheets that are sent home with young children, there is notification of future events like photos, and much more. The purpose of all this information is to provide a rich communication channel, but instead just leaves parents incapable of attending to changes, updates, and salient information.

The secondary effect of the sheer amount of information in the environments is that it is difficult to determine what the degree of sensitivity of this information. Additionally, what is one small piece of information, such as a record of bathroom successes, can start to add up to a rich story of that child’s life when it is all combined.

Design Implications:

- Simplify the information in the environment for parents to be able to attend to the salient pieces.

Child-P01 Observation Notes:

*2009-10-13 5:05PM I make my first stop at the Blue and Aqua rooms, which are immediately to the right as you head down the “long hall” that’s across the lobby from the kitchen. The doors are side-by side, with a bulletin board and desk sandwiched in between (Figure 6). The doors, wall, and desk are littered with information--papers, binders, file folders for each child, and whiteboards. There are informational sheets, sign-up sheets, lists with the names of children, the teacher’s name, names of substitutes, classroom illnesses, birth dates, artwork, daily activities, and more... The types information that I thought might be considered more private are exemplified in Figure 9. On the left, there are three instances of daily activity logs, which sometimes contain the names of children and things they did that day. On the right, there’s a pin-up of the a daily schedule that identifies who opens and who closes, and when other significant activities take place throughout the day. In the middle, there’s a picture of a binder and a file stand that seem to contain information pertinent to each child. [I suppose the binder has old copies of the daily summaries we see in the leftmost picture in Figure 9, while the file folder may be what PT1 is talking about when she discusses the tax forms]. Regardless of what is in these last two, I feel afraid to look into them. There’s something about the binder that makes it seem less public, even if*

*it is out on a relatively unguarded desktop. I'd have to take it out and open it to look at it--a more visible action that might require me to explain to a passerby what I'm doing. The files, too, give me this impression. Actually, the files seem even more off-limits to me. I tend to keep personal information in my own files, so I already consider files to be for somewhat private information. The fact that there's a child's name on each tab makes an even bolder claim to their ownership--and my lack of ownership--of the information in the files. I want to know what type of information is in these places, but I decide not to look for these reasons].*

Child-P03 Observation Notes:

*2009-10-21 10:17AM The classrooms have a big notice board with the meal plan and weekly activity information. Beside the entry door, there is a telephone mounted on the wall. All over the wall, there are lots of forms. Most of them are printed and are related to emergency number, emergency procedure, emergency exit plan and route, playground schedule, instructions on how to cough. Allergy information is handwritten and clearly visible. information behind the door. (The allergy information is covered).*

### **9.72 Licensing Issues (Study 1)**

Observed:

- Child-P01 2009-10-14 10:40PM
- Child-P01 2009-10-14 10:50PM
- Child-P01 2009-10-14 10:52PM
- Child-P01 2009-10-14 11:50AM
- Child-P01 2009-10-14 12:00PM
- Child-P03 2009-10-21 10:55AM

Interview:

- Child-P03

Licensing is the state-mandated process for regulating that childcare centers are managing the child and the child's information in a timely and confidential manner. There are really two incidents that demonstrate this process that occurred within Child-P01 and Child-P03. The licensor for these sites is the same person, PD1. PD1 primarily works from home and she drives to different centers to do scheduled and unscheduled visits where she tours the childcare center and then looks at a random ten percent of child and staff files. Any citations she writes up in her computer and then these are posted on the DSS website. An example from Child-P06 is included below taken from the DSS website:

*Facility Type: Child Day Center*

*License Type: Two Year*

*Expiration Date: Feb. 21, 2011*

*Administrator: Child-P06 Director*

*Business Hours: 7:00 A - 5:45 P, Monday - Friday*

*Capacity: 130*  
*Ages: 1 month - 12 years 11 months*  
*Inspector: PD1 Kimbrough, (276) 676-5629*

*Inspection Date: Sept. 17, 2009*  
*Standard #: 22VAC15-30-610-D*

*Description:*

*The last evacuation drill noted was for the month of April 2009. Theses drills are required to be done monthly.*

*Action to be Taken:*

*We will use the monthly desk calendar as the reminder to perform the drills. We will pre-mark the calendars now and continue to do so for the upcoming years to ensure compliance is maintained. We will also conduct 2 drills per month, for a few months, to ensure the children/staff are familiar with the process.*

Parents use the reports from the DSS website to determine the quality of the childcare center. For this reason and the gravity of not receiving a license to care for children, the licensing process is taken very seriously.

In the first instance, Child-P01 is visited for an unannounced inspection. The observation notes from what happened are included below. The synopsis is that the inspector observed three issues that should have been noted in the report: chemicals in a cabinet that are not locked, files were not updated, and purses were accessible. Part of the reason that this childcare was not written a citation could be attributed to the prior relationship that PT1 and PD1 have. It is revealed through the day that PT1 and PD1 used to work together before PD1 became an inspector.

In the second instance, Monika was observing PP2 from Child-P03 as she went to a room to make sure that the teacher was up to compliance with her licensing issues. PP2 notices many problems and makes the teacher aware of them. What is particularly interesting in this case though is how PP2 has a condensed one-page list of issues that she should attend to compared to the three-page list that is provided by PD1. The difference between official policy and local policies is highlighted in this. Similarly, PU1 from Child-P04 contacts her licenser to determine how to instantiate policies. She says, "I tend to, you know 'this is what it says and before I deviate from this, you know I'm going to ask someone. I'm reading it this way is it really ok to do it this way?' So, there's a lot of times I'll call the licensing specialist and get her opinion."

In this case the breakdown comes from confusion over what is the official policy and the negotiated in situ practice. Or, to say this another way, the difference between the explicit policies from the department of social services and the implicit policies of what is necessary to be passed for certain situations and licensors.

Design Implications:

- Create methods of documenting citations, but also areas of improvement that only are available for the childcare center and inspector

Child-P03 Observation Notes:

*2009-10-21 10:55AM PP2 is going to do a state license requirements check for one of the classroom. I follow her. Each class must be checked once a month to make sure that they are up to date. This information is used only by the center. The state does two big inspections in a year. Next one is in February. This inspection is about a list of information and things that must be present at each classroom like emergency information and up-to-date USDA information. PP2 gave me two forms, one which the actual state form, another one is the compressed version of the state form which PP2 uses. PP2 tells me that the state one is 3 pages long which make it complicated to work with. It also have some fields that don't apply to all the classes, the compressed version does not have those fields.*

Child-P01 Observation Notes:

*2009-10-14 10:40PM "so you keep all the medication, except for what I saw downstairs, up here. Is that right?"*

*"yeah, we keep the emergency medication down in the classrooms, like the EpiPens, because we want them to have direct access. So, they have that, but the medication form's kept up here. The EpiPen form that lists their allergy, that's always down there."*

*"so, it's like there's one in each classroom, basically, with the children who have the EpiPen are MAT certified or PMAT certified?"*

*"Yeah, we try-ee- <makes a non-sensical sound here to signify that her words are garbled, and she starts again> We have, PT3 and myself and PT8 and PT5 are MAT certified, and then we just had literally, on Tuesday night, had a PMAT class come through, so we hit those teachers that, you know, didn't quite have it, to make sure that they have it."*

*[I wonder if this means that the other teachers got certified or not. It seems like PT1 is being intentionally vague, but perhaps I just don't understand what a "PMAT Class" is--perhaps you can get MAT certified in one class? Google doesn't help much in solving the mystery.]*

*"OK, because the children have to be in care by a staff member who can administer, who's PMAT or MAT certified. Does that make sense?"*

*"mm hmm"*

*"Benadryl, or non-emergency medicine, as long as there is someone on-site, at all times. But, for the emergency medicine, if you're gonna keep it in the classroom, someone in that classroom needs to be certified to be able to administer it"*

*"Ok, so if the child was in there... are you saying that the child can be in the classroom with a non-PMAT teacher as long as I'm holding the medication, because I have it and keep it up here, is that what you're saying"*

*"because you would be the one to administer it, but if it was in the classroom, you run the risk of it being administered with her."*

*"because, what typically... before they didn't have it, we were like, this is what you need to do 'call us, we'll come down there, immediately', so the EpiPen's already down there, I don't have to stop here, I can just go down there, that's kinda what I was thinking, so, ok"*

*"um, well, before I leave, we'll weed through it and see what it says. I know for non-emergency medicine, as long as there's someone on site, but let me see what it says about the emergency. It might be a general overall, but I just want to double check before we change things."*

*"cause that could be just a fault on my part"*

*[there's a large pause (15 seconds) in time here before PTI clarifies her position with "but, nonetheless, they have it now." My impression is that he was churning through thoughts on the topic. This seems to indicate yet again how concerned PTI is in maintaining the reputation of the center.]*

*"but, nonetheless, they have it now"*

*"yes, will excellent"*

*2009-10-14 10:50PM "ok"*

*"but the only thing is that it would need to be out of reach and locked up-- it couldn't be just in her purse on the bottom shelf, you know. 'cause like, in the toddler room, I think it was in the toddlers cabinet, the white cabinet where the sink and the main stuff is, we had a purse on the bottom. Um, you might want to visit that and see if they could not place it in a toddler cabinet, just because I don't want to have to go through their purses to find out if they're carrying medication or anything that would be harmful to children, because that gets a little touchy."*

*[it seems like this comment might not have come up if the conversation hadn't turned in this way. It shows me that human convention (e.g., not feeling comfortable digging in someone's purse) sometimes trumps official policy (e.g. the job of the inspector to report harmful substances in reach of children). It also shows how exceptions may be made on a personal basis; would the inspector have been more persistent if PTI was less amiable, or if the childcare had more violations?]*

*"yea, yea" <very softly>*

*"so, it's better if we don't have to question whether or not there's anything in there that can be harmful if it's within reach and not locked"*

*"got it, I will go revisit that"*

*"some of the other classrooms, I noticed it was up higher, I'm thinking it was... who's the blond hair, really cute hair cut?"*

*"really short cut? N\*\*\*\*"*

*"Ok, she had that little pretty girl with her in the classroom"*

*"african american? mm hmm"*

*"um, I was gonna say 'mixed', but yeah"*

*[I consider PDI to be a bit of a 'country bumpkin' because I associate this terminology with racism, and I associate racism with low SES and growing up in the country. I notice that I don't like her very much.]*

*"I think it was their room, I'm thinking"*

*"ok, I'll tell everyone, so we'll find out eventually"*

*"just because I, you know, then you get into the fact that we have to question what's in their purse and I don't..."*

*"I understand"*

*"well, we go into people's homes, as we said, I don't want to have to go into somebody's purse, you know?"*

*"gootcha"*

*2009-10-14 10:52PM Another question from PDI*

*(ObservationP1Oct14.mp3, [01:17:12.16]):*

*"and, you've got your emergency documents on there for your bus and your van route?"*

*"emergency documents being...?"*

*"who you're transporting, sign in sign out, emergency information, first aid kit?"*

*"first aid kit's on there, notebooks with all the contact information's on there [except for <child>! this is missed]. They have a list downstairs [at the desk of PT8 or PT5?] the other of messages as well as up here that they check to cross-reference with their cross-off list of who to pick up, as well as their phone numbers. They do not leave the school until they contact <inaudible> despite the school saying 'yes' they were a car rider"*

*"do they keep a list of who's on there at the given moment, like a check off like 'we have 16, and it's Johnny, Jane,"*

*"They have a laminated list, itemized per vehicle as well as--I wish I had it handy--but a laminated list with all the children's names on it that they can use a white erase marker, and cross off who's not supposed to be attending"*

*[I'm still not sure this complies with what PDI is pressing for]*

*"and, you know part of the back up reason for that..."*

*"I'm assuming if you get in an accident and the driver's unconscious--"*

*"the police would need to know--"*

*"who's on the vehicle"*

*"and who to look for if they're not on there"*

*"that's what I tell my little friends--'it is not about just attendance, so yes."*

*"you know, and there's no nice way to say that, except for I just tell people 'if you can't speak for yourself, they need to know whether they're looking for 20 children or whether you only have 5 today', so you need to have a list of who's on there at that given moment."*

*"yup, I typically respond with 'I'm glad that you have a great memory, but when you're unconscious you can't tell it."*

*"yeah, very good"*

*"yeah"*

*"see, like minds"*

*[PTI in her quest to create common ground]*

*"well, it's just all these years of knowing and seeing what happens, correct?"*

*"yeah, unfortunately"*

*"unfortunately"*

*"and plus, they do a count, but they like walk through the bus and make sure everybody's off?"*

*[this seems like a terrible way for licensing to actually check to see if this is the protocol. 1) asking, not observing, 2) leading question that hints at the right answer]*

*"mm hmm"*

*"ok"*

*"yup, that's on our van rules which are also posted on the vehicles"*

*"alright, and then they sign off that they've done a final check?"*

*"I don't necessarily have them sign off on it"*

*[does she need to have them sign off on it?]*

*"ok"*

*This last conversation was a little bit of a struggle for PTI. She seems to know that they are not implementing all the procedural requirements on the bus. None of the explanations she has given me or even PDI here have included a current count of who is on the bus. And, there's apparently no sign-off to signal that no children are on the bus after the route is complete. PTI's answer to PDI's questioning of whether this last check even takes place--regardless of sign-off--seems a little nervous and unconfident. In her roundabout explanation of the cross-off list--which avoids directly answering the question--PTI admits that there is not a count/list of who's on the bus at any given moment without directly saying it. PDI responds to this by providing the background explanation to PTI of why it's important and leaves it at that. There might be a misunderstanding, where PDI thinks that the procedure is actually in compliance, but her other behavior leads me to believe that she is probably just passively making PTI aware of the correct procedure and then ignoring the infraction. PDI has already noted the purse on the child-accessible, unlocked shelf and how she dismissed closer inspection for social reasons. We later learn that she overlooked a can of spray chemicals in an unlocked cabinet in the art room, and an unprotected outlet. Finally, she was made aware that files were not fully updated and said that she would turn the other cheek as long as she didn't see PTI actually updating the files. In the end of the day, no violations were reported in the final write-up.*

*2009-10-14 11:50AM PTI goes on to explain (what I assume is said in the \_\_\_ above) (ObservationP1Oct14.mp3, [02:18:39.01]):*

*"I was updating files, I was like 'I really shouldn't do this while she was here'"*

*"she already left?"*

*"yup"*

*"wow"*

*"we're clean, but, pass the word. She had to lock many a cabinet. Your cabinets that were unlocked thankfully didn't have chemicals behind them. The art studio did. Someone went into the art studio--PT7 had silicon \_\_\_ spray or whatever to put over, and it was locked in a cabinet--and <very quietly> they left it unlocked and so she pulled it out"*

*2010-10-14 12:00PM "did she go through files, too?"*

*"no, because she went through them last time, so. When I was sitting down, I started to go through the update, and I was like 'I have a stack of 20 here that aren't complete' and I knew she wouldn't call me on it, she was like 'as long as I don't see 'em, 'you don't let me physically see them.' So, then I was like 'ooh,' so I'm sitting there working a batch that I don't even have to be putting together--I don't have to do a \_\_\_ batch, so I'm like, 'I'll just work batch'"*

#### Child-P03 Interview Transcript:

*PP1: And I guess there is some variations on that anywhere you go. Umm, I know my licensing agent is not the one that my friend Tina has in Dublin. And she is being written up for things that my inspector does not write me up for. Umm, you know... umm, because, my inspector was a childcare director at one time, she has done my job. So she tries to be.... she reads the standards, she follows them, but her interpretations... they are...the standards sometimes are left open for interpretation, which can..... there are times that my friend went toe-to-toe with her inspector because she doesn't <38:03> agree with her version of what it said.*

### **9.73 Incorrect Beliefs About Technology (Study 2)**

Observed:

- Med-P15 2010-08-26 1:16PM

In the example below the doctor from Med-P15 is upset at PC1 because he believes that PC1's access of Facebook is the reason why their computer is no longer working. He believes that she downloaded a virus from Facebook that has now crashed the computer fatally. This example is important because the computer hosted a large amount of patient information. His concern though was not about the fact that information had been lost, but about the cost of the computer and the time.

Design Implications:

- Create technical systems that do not allow for other online browsing.

Med-P15 Observation Notes:

*2010-08-26 1:16PM This issue with the computer is kind of interesting. I mean, a new computer only cost a couple hundred dollars. I don't know*

*why it is such a big deal to get a new one. It then occurred to me that it is because they don't have the know how to transport all of their old settings to the new computer. Until it is fixed or replaced, it is just sitting there unused. I asked N at some point, maybe later in this same day, what is the problem with the computer. She says it wont even boot into DOS but that the motherboard isn't beeping. It sounds like the memory is corrupt, but I'm not going to offer to fix it for them. It later comes out that the doctor thinks that the reason the computer died is because PCI was on Facebook. In this case, he is continuing to give her trouble about how other people are using the computer that is supposed to be 'hers'. So she fights back by telling everyone to stay off of her computer - to highlight how little work will get done.*

### **9.74 Incorrect Beliefs About Technology (Study 1)**

Observed:

- Child-P01 2009-10-14 11:00AM

Interview:

- Child-P12

There were instances where the people who worked in childcare centers and physicians' offices had incorrect beliefs about security and technology. These breakdowns are specifically noted together because I found that many of the people in the study have not adopted electronic records because of a fear of technology and an unwillingness to learn new tools.

In the case described below PD1, who is the licenser for many of the childcares in the study, is talking to Stacy about security. She explains that the reason she does not use a password or engage in higher security for her computer is that she believes that all security is negligible. If a "hacker" really wants into her computer he is going to get into it no matter what she does. In the second case, PV1 from Child-12 believes that because her online web-camera system is less findable because it is not connected to her childcare center's website.

These examples illustrate not just incorrect beliefs about security, but demonstrate a lack of knowledge of how technical systems work. In general, it demonstrates a large lack of real knowledge of who is the treat in the security model for these centers.

From an Activity Theory analysis, there is simply a lack of a rule surrounding security. This means that personal beliefs - incorrect beliefs - are the ones that govern how sensitive information is going to be managed.

Design Implications:

- Provide visualizations of the security threats for different technical systems.

Child-01 Observation Notes:

2009-10-14 11:00AM "Because the office is in Abingdon, which is an hour and 40 minutes away from me. And, because I service this area, I kinda have a satellite office out of my home because I have remote access now that we're online. So, we've got password protection--there's password protection for everything--they're like 'don't write it down', I'm like 'excuse me' <inaudible> if somebody really wanted what's on this computer, it's not gonna give them, I mean, they'd have to know how to navigate the system which, is not the easiest thing to do... but there's really nothing on here. I mean, I think they could get on other programs that we don't use, possibly. But, if somebody really wants on they're gonna be smart enough to get on it, whether I have a nice long 12-letter multi-digit pass code or not. I mean, if you're a hacker, you're a hacker for a reason, and with our systems, I mean, I'm sure there's other information with other agencies that are more prudent than our little licensing stuff. But, nonetheless, that's a concern. They're always concerned about, you know, confidentiality of stuff. I'm just like, it's the same thing with anything else, if they want it bad enough--"

"they're gonna get it"

"whether your doors are locked or whether they're unlocked, if they want it,"

"they'll just break the window, right?"

"they're gonna get it, you know, that's just how it is. People become smarter and smarter and do things to make themselves be able to do certain things for a reason. So, I'm not one of them, I don't do online banking, I don't trust any of that, I mean I just don't, I don't pay bills online, I don't do any of that because I don't trust that someone can't just come right in and scoop it up. I didn't grow up in the computer age, so I'm wary of--in college we didn't even have computers, we still had typing lab the year I graduated from college. The year after they had a computer lab all of a sudden, so I'm not in that, and I get so mad when this doesn't work, so now what. How am I supposed to do my job? Whereas before I could do it because we have paper. And they're like, 'well you can still use the old way and go out and do it,' I'm like 'no' because then I'm gonna have to redo it to put it on here."

PT1: "makes it double work"

me: "it does, yeah"

#### Child-P12 Interview Transcript:

P12: they can access the webcam.. so they have - each child is specific to their room so, if you had a child that was in the toddler room they would a password specific to the room, not to the whole center.. so they have access to the room their child is in

Tom: and they use like an online portal to get to that?

P12: yeah, mmmhmm, and it's not connected to our website so that it would be harder to hack

## 9.75 Difficulties Communicating with Foreign Parents (Study 2)

Observed:

- Child-P01 2010-08-31 1:27PM

The information exchange between care provider and parent is important for handling the daily care of a child. If a child did not sleep well the night before the message will be passed on in the morning. Any difficulties the child had that day will be discussed in the evening when picking up the child. This exchange allows the two people to coordinate on what issues the child needs to work on, what the child is doing well, and how to proceed.

In the breakdown discussed below, all of the administrators for Child-P01 are in the director's office having a team meeting. PT5, who is the owner of the center asks about a particular room, and PT6, who is a part time administrator and part time teacher in that room, responds that she is continuing to have problems with a young Asian male student. The problems is that he does not do well with discipline, he acts out, and he expects his care worked to do work for him instead of taking care of himself. PT4, who I believe is Red-Shirt in this snippet, also chimes in that he has had similar problems in previous classrooms that he has been in. This is said to discredit any objection that it is just that room or a recent problem. Eventually, what emerges is that the teachers have tried talking to the mom, but she speaks very little English. The teachers have tried using the little boy, who speaks both languages, to function as a translator, but that has not worked either. So the teacher stands there explaining how the little boy has "areas to improve upon" but they do not think that she is getting the message.

The communication breakdown creates a barrier for the development of the child. This has resulted in not only the student being a point of discussion with the administrators and teachers, but additional people having to be pulled into the issue such as a translator. It has become hard for the childcare center to respect the privacy of the family's situation when the child is so badly behaved, and they cannot correct the behavior of the student because they cannot communicate with the parents.

Design Implications:

- If documenting behavioral milestones or problems, have a pictorial representation.
- Provide labeling/displaying child information in multiple languages.

Child-P01 Observation Notes:

*1:27 PT2 brings up that B\*\*\*\*\* will be back to volunteer on Tuesdays and Thursdays. PT5 asks if PT2 will talk to A\*\*\* and A\*\*\*\*\*o about it. PT5 asks PT6 about another room. There is a student with a mother who doesn't have much English and the little boy is walking all over her. PT5 raises the issue of cultural differences. Red-Shirt says that the little boy is impulsive. PT2 asked about how many days he is going to come in. Red-Shirt says that she pushed the mom to have 5 days since she is pregnant. PT6 says there was a problem with the young boy in a previous year. PT5 says that they should have a parent conference early. PT6 says that they'll*

*need a translator. PT5 says that what they can get is a translator for written stuff. PT7 says that she has a workbook with a worksheet: 'Ten languages that every preschool teacher should know'. It allows them to hand foreign parents information sheets. PT7 says that she'll bring them in. The problem here is that the son is a bit of a terror in the classroom. They talk about how he demands to be waited on and have everything done for him. Since he has been around for a while now, they've watched him from room to room, and the behavioral problems persist. The ladies speculate that it has something to do with him being Asian, and an Asian boy. Never the less, the problem is that the mom does not speak English. The teachers and staff have problems communicating with her about the behavioral problems with the child. They ask him to translate for them, but for all they know he doesn't actually repeat what they are saying.*

### **9.76 When Staff Does Not Document "Adequately" (Study 2)**

Observed:

- Child-P01 2010-08-31 2:37PM

Childcare centers have varying policies on documentation. While some documentation is required to be licensed care provider, such as when accidents occur, most policies governing when something will and will not be documented are local. For instance, some childcares like Child-P04 and Child-P01 document weekly developmental milestones that the child is meeting such as stacking blocks or sharing in a new way. These are then stored in books that the center shares with the parents, and for Child-P04 with people who may be running experiments on the children.

Within Child-P01, there was a discussion during one of the administrative meetings about a teacher who was not working on her "Me Books". Me Books are books that are made for each child with pictures and stories of how the child is playing. Or, to use a phrase from the director, "To a child, playing is work". The Me Book documents the work of children to make sure that they are progressing and to allow the parents and teachers to discuss issues related to the children. Given the number of children in each room, this documentation can be a large amount of work. In the observtation, an office staff person talked about how it is important to do a little bit of this documentation each day, and to also give yourself a set amount of time for each book – such as 30 minutes. This focuses the work and makes sure that it does not start to pile up.

The problem discussed in the observed meeting is that there was a teacher who was not working on her Me Books adequately. PT7 says that this teacher has not worked on her Me Books since March, which at the time of this observation was seven months. Prior to March there was also an extended period of time before the teacher had worked on her Me Books. PT7 said that the teacher was working on her Me Books and spent ten hours working on one book. After all of this evidence, PT5, who is the owner of the center, said that the teacher should be "pulled" from the room, meaning that she should no longer be a full time teacher in charge of tasks such as documentation.

While there are other issues with this teacher, it highlights the importance that this location places on documentation. In this case, documentation means more than the sterile documentation of a child, but also the social and developmental aspects of a child's growth. A space for this kind of documentation, which has much more private and nuanced information than perhaps even a medical record, is not currently supported in any way with an electronic system. Although it may be suggested that there is not a need for this information to be made electronic, in both Child-P01 and Child-P04, both of these centers start their documentation as an electronic Word file. The sharing is then facilitated through printing the document and putting it in a book.

Design Implications:

- Allow for documenting more social and developmental information about a child, and then sharing this information with parents.

Child-P01 Observation Notes:

*2010-08-31 2:37 PT7 asked if <owner> wants here there for the meeting with <teacher>. PT7 explains why she is frustrated - which is that she hasn't done her Me Books since March. A parent talked to PT7 today about how her Me Book hasn't been done in months. <owner> says that she needs to be pulled out of the room and just be a floater. PT2 says that she is always trilling and gossiping instead of talking - which isn't fair for <Child-P01> to pay for that time. <owner> says that PT7 needs to sit down and watch her do one. PT7 said that <the teacher> says that she took 10 hours to do one.*

### **9.77 Client Information is Permanent (Study 1)**

Interview:

- Med-P02
- Med-P03
- Med-P04
- Med-P05
- Med-P07
- Med-P08
- Med-P09
- Med-P10
- Med-P11
- Med-P12
- Med-P13
- Med-P18
- Child-P03
- Child-P04
- Child-P06
- Child-P10

For all of the physicians' offices except for Med-P01, Med-P06, and Med-P16, who only reported kept their client's files for seven to ten years, all offices reported that they kept

both their physical and electronic files indefinitely. As for childcare centers, there was a similar trend to keep certain children's files indefinitely as well.

Reasons provided for keeping the files for so long were in case the electronic file crashed – there would always be a back-up; because the director/owner reflected that the files represent his “life's work” and he did not want to destroy it; because the center was unsure what else to do with the files; in case the center or doctor was sued for mal practice; to support the community - to be able to identify dead bodies; because they believe there to be a law stating that they need to keep the files that long; because the director does not feel comfortable being the authority for deleting the files; and, because the system will not let anyone delete a file – only mark the patient as in active.

When a patient provides their information, it is unlikely that they consider that their information will permanently be stored in that location. All of the parent in this study believed that after their children stop attending the childcare; their files will eventually be disposed of. Parent-P12 mentioned that her daycare said that they will dispose of the file after six months of her child's leaving. No other parent could remember any other date. In general, clients probably assume that after a reasonable amount of time their file is deleted. In essence, clients assume that their information is a has the shelf life of their business, thus not requiring the centers to manage that information after a certain period of time. However, this assumption is generally false.

Medical files and child files are much more permanent – especially if the client is difficult or left the center under unusual circumstances. The director from Child-P03 talked in her interview about an incident where a teacher placed a piece of tape over a child's mouth who would not be quiet. Not only is the teacher's information going to be permanently kept on file, but so is the child's information in case of a pending law suit.

The breakdown in this situation occurs because there is a lack of a visible rule governing the limitation of how long a client's information can be stored. This highlights an ambiguous situation that allows the clients to continue blissfully unaware, and for the centers to continue managing and storing client information however they want.

#### Design Implications:

- Periodically remind clients that their information is still being stored at a certain center
- Create files that auto-degrade after a certain amount of time.

#### Med-P02 Interview Transcript:

*Laurian: Okay. How long do you keep your records here?*

*PQ1: We keep them 7 years; we have a file cabinet upstairs for the ones that haven't been here in the last 5 years but we keep them for 7 years.*

*Laurian: Okay what happens afterwards?*

*PQ1: Well actually Dr. Glasgow still has them. He has them from when he started 20 years ago.*

Med-P03 Interview Transcript:

*Laura: How long do you keep the hard copy files?*

*PF1: He's been in practice for 6 years and every patient is still here. I don't know beyond that. He may say after 10 years get rid of them. We have a lot of people that just come one time, so.*

Med-P04 Interview Transcript:

*PG1: No ma'am. My father was a chiropractor, so his first clinic was in Pulaski. It's 30 years old. And then actually one of his clinics was purchased by him in 1982, and that's been open since 1930. And then I bought another practice a couple years ago and that's been in practice since 1972 or 3. So we've got, and then we just opened an office about 14 weeks ago in Cave Spring, so that's brand new. So we've got everything from 70 some or almost 80 years to 14 weeks.*

Med-P05 Interview Transcript:

*PH1: Well we have an inactive filing system in the basement, and then you have to keep them for a minimum of 10 years from their last office visit so we now hook up with a company, shred it, and after ten years you can shred it, but you have to keep it for at least ten years. Ten years after they have been an active patient so that's really more like 12 years. Because we may see them for a few years before we call them inactive. The problem is, and someone wouldn't think about why it's so important, but it's like the Virginia Tech massacre we had 3 patients who we had to identify the bodies with dental records.*

*Laura: So it's a good thing that you had those files.*

*PH1: Yes. Right. And we actually had to dig into our archives for a Tech professor that died in a plane crash maybe 10 years ago, and that's the only way they could identify him was from dental records.*

*Laura: Right, yeah that makes sense.*

*PH1: So you know after 10 years sometimes I get nervous about getting rid of them then!*

Med-P07 Interview Transcript:

*Laura: Okay and can anybody add, modify or delete information?*

*PJ1: You can't delete anything. Once you put somebody in there they're in there for good. We can make them inactive, but you can't delete them.*

*Laurian: Okay so after the 10 years what happens to the patients' information?*

*PJ1: Oh in the computer, it stays. It's always there. We make it inactive so that when*

Med-P08 Interview Transcript:

*P11: We just started purging and we have to keep them at least 7 years and we have a little more than that. I think we just started getting rid of 2000 and further back.*

*Laurian: Why do you have to get rid of them?*

*PII: For space, and for people, a lot of them don't come in anymore, so if they don't come in after 7 years then they're not coming back.*

*Laurian: So what happens to them?*

*PII: Um I think they were, actually I'm not sure. They were thinking about burning them or getting them shredded but I'm not sure what they decided to do. I think right now we've got them just in storage in another building.*

**Med-P09 Interview Transcript:**

*Laura: So you've been here 18 years, and there are at least 18 year old files in the storage unit?*

*PK1: A little bit more. I guess 20 years.*

*Laura: Do you think you'll ever shred some of them or go through them?*

*PK1: No we even have the deceased; we don't get rid of anything.*

*Laura: Is there a reason for that?*

*PK1: well for example, we had one patient who was deceased whose family there was an incident at a local hospital having to do with their eyes, a cord or something that was draped over their eyes when they were unconscious. So the doctor had to go up there to see them and the family was suing the hospital so they had to have copies of the records, so there was like, and we have a lot of patients who move away and come back and we'll still have their records.*

*Laura: So the files that are out here, are they 1 or 2 years old?*

*PK1: They're more current yeah. We have 4 years up here, 4-10 in the back and the rest are in storage.*

**Med-P10 Interview Transcript:**

*Laura: How long do you keep them?*

*PL1: I have yet to throw a file away. So I have 17 year old files in there.*

*Laura: What all goes into the file?*

*PL1: Name, address, phone number, pertinent eyeglass information, a copy of their prescription, the frame and the price.*

*Laura: Okay so if someone's been coming to you for 17 years and gets a new pair of glasses from you every year, their file is pretty thick?*

*PL1: Oh yes.*

*Laura: All right and they're all still in this building.*

*PL1: Yes*

**Med-P11 Interview Transcript:**

*Laura: How long do you keep the paper files? So I know you've been in practice 7 years, are there 7-year-old files here?*

*PM1: There are, but we actually do keep all the files, the documents that are pertaining to that. There are certain, like the EOB's from the insurance companies that only need to be kept a certain amount of time, so we won't keep those.*

*Laura: How long do they have to be kept?*

*PM1: I think 6 years.*

*Laura: Are all the files stored in this building?*

*PM1: Again because of the HIPPA thing they're really not allowed to leave the building.*

Med-P12 Interview Transcript:

*Dr D: Yeah. At the hospital. Well both places have only had electronic medical records. Well here it's been 2 years, so the hospital may be 3 or 4 and it's all kept. And I think it'll probably all be kept indefinitely. As long as it's feasible. Legally you're liable from a malpractice point of view, you're liable for 2 years past the point of discovery.*

*Laura: 2 years from when they first come in?*

*Dr D: From the point of discovery. So if you have surgery and then 6 months later you discover that they left the sponge in your abdomen, then from that point forward. But if it's a child it's 2 years beyond their 21<sup>st</sup> birthday. So if you leave a sponge in a 2 year old and it's found out when he's 18, you're still liable. So you gotta keep. For children you gotta keep records for a long time. But I suspect the storage will endlessly increase. Because it used to be such a problem- we used to keep medical records here before the electronic medical record. We kept them here for 2 years and then took them to a storage facility because we just don't have the room. But then getting them is always such a problem because they get put in some storage thing somewhere, and then if you want it you gotta move heaven and earth to get it.*

Med-P13 Interview Transcript:

*Laura: How long do you keep the patients' paper charts?*

*PN1: 10 years.*

*Laura: Have you ever thrown any away?*

*PN1: Well we've been open for 2 years*

*PN2: We've never had to throw any away.*

Med-P18 Interview Transcript:

*Tom: Okay, you keep the patient files for one year?*

*PO1: After they are discharged. Well, I don't want to say this. We are required to keep them on premises for a year.*

*Tom: Okay.*

*PO1: And then we transfer them to a storage facility.*

*Tom: And you usually keep them indefinitely after that?*

*PO1: Depends on, umm, minors we keep indefinitely. Adults we keep six or seven years. And then they can be destroyed.*

Child-P03 Interview Transcript:

*PP1: No, I ....The only time we take something out is...No, actually we cant terminate it, we cant destroy anything from the file. We do, and the state actually requires annual updates. So this month, I have got to send*

*out brand new registration forms and the USDA requires manual updates. So, they are gonna get another pack of paper to take home, refill this out again, and it goes into their file but I cant take out the old stuff, it has to go in with it, it's ...just... cause you are not allowed to destroy anything in a child's file. And that's the state thing so we just keep <8:52> accruing lots of paperwork.*

Child-P04 Interview Transcript:

*Interviewee: "As long as they're current employees or current children, they stay in here. Once they leave, they go into a new file, which is in another area that stays locked. And, if your followup question is 'how long it stays there, I've been told 3 years, but I have not gotten rid of anything; I've been here 5 years and I have not gotten rid of anything. I'm going to let someone with a higher authority make that determination."*

Child-P06 Interview Transcript:

*Interviewee: staff files we keep physically for current employees, now children and staff - once they are no longer employed here or no longer enrolled here we do take them - we box them up and they are taken to secured storage*

*Tom: so there's an offsite place for information?*

*Interviewee: yeah, for previous families - i mean they're all accessible but, because the center has been open long enough, we just don't have the physical space to keep that many*

*Tom: so how would access to that work?*

*Interviewee: i've not been to the storage facility yet.. right now the people who are the owners of the program are mainly the ones - when a box gets filled up i call them and tell them and they come and take it for the storage facility for us so they would have access, i would have access - we have an assistant director and if she had a request then she probably could but beyond that there's probably not going to be other people*

Child-P10 Interview Transcript:

*Interviewee: no right now we keep them here and we are working on now how we are going to store those things because the new building we're going, we do have some room where we can put filing cabinets in that can be the archives but it keep growing so we don't know how long - because Pathway was actually a merger of two schools so we have - and both of those schools were in existance for over 20 years so we have files from both of those schools and usually they end up in my office*

*Tom: so is keeping old files sort of a policy from the licensors? or is it just something that you guys do?*

*Interviewee: well actually, like public schools too they have to keep those kinds of things because we had - just last year we had somebody call and they were, it was an employee file and they were employed here like 12 years ago but they needed information that was in that file and we had it -*

*student files we have, I believe, that's a mandate that we have to keep the files... I would think that we'd only have to keep them for 10 years or something like that but it's not, you have to keep them*

### **9.78 Situations Where There is a Need to Disclose More Information than “Normal” (Study 1)**

Interview:

- Child-P03 (2 instances)

In the childcares that were interviewed and observed social methods were used to control information flow. In general, teachers were not allowed to have access to all information, and in some cases (Child-P01 and Child-P04) the parents could actually restrict this access themselves. One social method that directors used was limiting the amount of information about a child's family circumstances with the teachers. While teachers have the most access to the child, there were times when the director at Child-P03 felt that teachers did not need all of the information. These include when parents were getting a divorce or if a new child was entering the center that had a biting problem.

I provide these cases to then juxtapose them from cases where PP1 felt the need to provide extra information to the teachers. The first case she explained was when foster children are attending childcare. This is because she wants to make the teachers hyper vigilant to make sure that the child is not being picked up or talking with someone in the playground who is not their foster parent. In this case the extra information is to provide an increase in security of the child. The second is in cases of custody battles between parents. She explains that there can be times when a parent is deigned custody to their child, and they will try to gain access into the childcare. Making teachers and others in the center more aware of this family situation can also provide an increase in security.

The breakdown here is represented by the fact that electronic systems do not provide “special circumstances”, or places in a file where more access to that information could be made available. It would be great to envision a system where a custody agreement has changed for a child, this is documented in the electronic file, and a notification is pushed out to the rest of the center. Instead, this information is documented in the electronic system and then disseminating the news relies on the social system.

Design Implications:

- Support laying information such that at times more people can have access to information and at other times the information is not as available.
- Evaluate what information that is kept on a child is related to their safety (e.g., foster status, custody status).

Child-P03 Interview Transcript:

*PP1: Umm, I have had, <20:16>, when we have foster children, I do feel like I have to tell them, that's not mom-that's foster mom. So, you have to be a little more careful when you are out on the playground, you watch for strangers, because that's, you never know, you know. I do, tell them*

*thing's like that, but...I am... it's according to what it is, if I feel like they need to know it or not.*

*PP1: So, when I, when their file... because we can scroll up and down using this, well if I see a screen that has that, you hit that and it's gonna tell you. So, we do that for families that has a custody agreement where a parent cannot come in. So, if, ... a man shows up at the door, and you know, we do have a security system but that doesn't mean you can't lie at the door, 'Yes I would like to enroll my child and I have some questions', you get them through the door and go 'actually my kid is here, and I wanna know where they are at.' Or I can't know that if you lie the door.*

### **9.79 Filling in Missing Information (Study 1)**

Observed:

- Child-P03 2009-10-21 10:15AM

There is some information that the state requires for licensure purposes to be documented for each child. One of these pieces of information is when a child comes in and leaves every day, and who that child leaves with. These files are audited by a licenser and can also be subpoenaed at any time by parents who are going through custody issues.

Given my experience with the three different childcares in the NRV area with my own child, I can say that this is an issue that is taken fairly seriously. A missing entry can cause the childcare to be “written up” – meaning that the information is displayed on a visible wall in the childcare center and it is also placed on the Virginia Child Services website for any parent to go and look at. I had always wondered what happened why the child's guardian forgot to sign in or sign out the child and the teacher also forgot who picked up the child. I know that there have been many cases where my partner has forgotten to sign in or sign out.

In the observation notes below, Monica was able to observe PP2 going over a sign-in and sign-out table for a particular classroom. She sees a cell missing and decides to fill it in based on her own memory, which I would argue could be fallible. The people at the front desk, like PP2, see relatively the same people day in and day out. I think it would be difficult to say that she remembered one day over the other, unless there was something unusual about the circumstances. Whether or not PP2 really remembered or wanted to make sure that the information was complete for licensing, this breakdown illustrates a case where the rule is regularly not followed. It is PQ11 for parents to forget to sign their kid in and out. However, the stakes for not doing this important step are not clear to the parents who are supposed to do the work. The obfuscation of the activity of licensure in conjugation of the activity of dropping off and picking up the child leads for latter activity to take prominence. This results in a breakdown, and breaking of the rules surrounding who should be documenting.

Design Implications:

- Create a method to highlight the importance of signing in and signing out – what the eventual goal is for this activity.
- Use social pressure for compliance. Provide a way for parents to see how poorly they are doing at signing in and signing out in comparison to other parents.

Child-P03 Observation Notes:

*2009-10-21 10:15AM PP2 was explaining this to me when she saw one blank cell at the day before. She filled it up, wrote down the time and the person who picked up the kid. She told me that she remembers who took the kid out from class yesterday.*

### **9.80 Menacing Outsider (Study 2)**

Observed:

- Child-P06 2010-09-02 9:34AM

This instance was the only observed case where anyone was directly concerned with security, and it is one time that was directly obvious. In this case, PE1 from Child-P06 is sitting in her office with me processing payments for the children. There are two men outside who are doing some landscaping such as mowing the laws, blowing leaves, and cleaning up the sidewalks. I'm watching them do this out the window and make a comment to PE1 about it. She says that one of them, the one with the red bandana is particularly menacing. He makes comments to women who work they as they come in and out of the center. The comments are not anything directly rude or harassing, but they the way he hangs around and talks to the women is a little creepy. She says that if she could, she would complain to do something about it, but as it stands she has not.

This case demonstrates a breakdown in social policy about men lingering around childcares. While the man's activity of talking to young women overrides the social rules governing not being creepy. In terms of the socio-technical system, this demonstrates the lack of security embodiment in managing sensitive personal information.

Design Implications:

- Support documenting people who are suspicious outside of childcares.

Child-P06 Observation Notes:

*2010-09-02 9:34AM PE1 comes back into her office. I was just noticing the people who are mowing the lawn. At the same time, PE1 does as well. She says that these two guys are a bit creepy. There is one in particular who is wearing a red bandana that she has had problems with. She says that when girls come in or people come to drop off applications she'll see that he tries to talk to them, and they walk a bit further away from him to try and avoid talking to him since he doesn't know anyone here. It doesn't seem like she is going to do anything about it, because the people who are doing the lawn service aren't hired by her, but she has taken notice of it. I think if she didn't feel safe, she might raise the issue with the landlord. It is more of an issue for the ladies, she says.*

## 9.81 Childcare Obscuring Information (Study 1)

Interview:

- Parent-P00
- Parent-P02

Some parents take accidents with their children very seriously. ‘Accidents’ when used in this way means that a child has been hurt in some way that results in harm to the child but not enough harm to result in a hospital visit. One type of accident is biting, which usually occurs in the children who are under the age of three. Usually in a classroom there is at least one ‘biter’ who is going through a developmental stage and biting other children in the room. This process can be traumatic for the children, but more importantly for the vocal and paying parents.

In the interview transcript below a parent discusses an incident where she felt that her daughter was being bit too many times – in this case more than five of six times. She felt that keeping the confidentiality of the ‘biter’ was not resolving the issue at hand. Instead she asked the teachers, some of who would tell her who the biter was, and started to discuss the issue with other parents. Eventually, by escalating the issue to the owners, teachers were moved in and out of the room, the child was moved, and the parent’s issue was resolved.

This case illustrates one of the few times when parents felt that they were not getting enough information. Usually parents felt bombarded with information as they entered the childcare to the degree that they felt it was difficult to attend to salient information. However, when it comes to the harm of their child, parents require more information that may infringe on the privacy of others in the room. In this case, the mother’s activity of protecting her child is in direct conflict with the center’s activity of protecting the privacy of the biter.

Design implications:

- Support parents being able to notice and discuss trends in classrooms.

Parent-P00 Interview Transcript:

*Laurian: and what ways do you communicate with them - is it mostly handed off?*

*Parent1: they take the information to the child's cubbies at the end of every day so we just pick it up when we leave... and in the case of an accident... they usually tell us verbally but not always... and if we request, which I do, if it's a bigger accident than a bump or a bruise then they'll call me every time*

*Laurian: you have to request that?*

*Parent1: I had to request that because there was a biting problem - she'd been bitten, I think, a large amount of times and so I said "from now on, you call me" and they do now... and I actually had to request being told verbally because they were just putting the accident forms up there and it's*

*kind of hectic at the end of the day since they've got a lot to do and a lot of parents coming in but I said "you need to tell me"*

*Laurian: ok, and when they called you and talked to you about the biting, what did they say?*

*Parent1: they just said that they wanted to let me know because I requested to know that <child> had been bitten again... that was all they said and I had to ask for more information*

*Laurian: and what information did they provide you?*

*Parent1: the scenario for how it happened*

*Laurian: did that change any behavior or anything that you did after that?*

*Parent1: yeah I was pretty upset because it was a whole biting incident and I went in and I said - this was the fifth or sixth time at this point and I went in and had a conference and involved other parents in the incident*

*Laurian: so what happened at the conference?*

*Parent1: well basically we let them know we didn't think it was okay that this was continuing to happen and they weren't doing anything about, we didn't see any strides or stubs - you know, not saying they should've taken the child out but we just communicated that they needed to be doing something... and then shortly after that I called the owner because I know her personally and I said "this has got to stop" and she actually went over and talked to the director and there were some changes made and it has been much better*

*Laurian: I know there's a new director there... was this before that?*

*Parent1: this was right in the middle of that... she came in on June 8th... <child> hasn't been bitten since she's been there but the biting was still going on*

*Laurian: So why do you think there's no more biting?*

*Parent1: I think, personally, I think that the child is growing up... there has been a few incident since then*

*Laurian: Did you ever find out which child it was?*

*Parent1: yes... they changed some staff, too... they moved a girl out and said that that might make a difference and they brought another one in... I don't know if it was because of the one they took out or if it was because of the one they brought in but we, as parents, really had to stay on top of that in a way that I don't think we should have*

*Laurian: Did you feel like there was information that they weren't providing you at some point?*

*Parent1: Some of the teachers would tell me who the child was and some wouldn't which I think the right thing to do would maybe be not to tell so I don't know*

*Laurian: So some of the teachers were telling you and some weren't?*

*Parent1: right... I never thought there was enough information either way about that*

Parent-P02 Interview Transcript:

*P2: I think, sometimes when I pick up her, like one time I notice my daughters face is uh, has a big scratch but the teacher told me that she don't know because she only comes here at three o'clock that it is the other so I have no idea. It looks like some teacher in the morning just come in late.*

*Laurian: So what happened with that. Did you bring it up?*

*P2: No. No. I just thought that maybe the next time I go to the other teacher in the morning. She told me when, if, when she came in she remembers the scratch already being there. But in my mind it is not. But I have no idea to say this. It is ok. After one or two weeks it is fine.*

## **9.82 Parents Not Knowing Who Can Access Their Child's File (Study 1)**

Interview:

- Parent-P00
- Parent-P02
- Parent-P03
- Parent-P04
- Parent-P08
- Parent-P09
- Parent-P14
- Parent-P15
- Parent-P17
- Parent-P18
- Parent-P20

Most of the parents in the study had not really considered who could access the information that had been provided within their child's file. While it may appear that there is a limited number of people who interact in a childcare, the list can actually be quite extensive. Within a single childcare there can be owners, a board or advisors, a PTA, directors, administrators, teachers, lead teachers, licensors, and others such as therapists.

When originally coding for this issue it was called a light-bulb moment because it was at this moment that parents usually realized that they had not previously thought about the issue. When probed, they had ideas about who should be able to access their child's file, such as their teacher or the director, but had no way of confirming their suspicions. This lack of knowledge directly reflects an accepted amount of ambiguity about how their child's files are being managed.

From an Activity Theory perspective this breakdown demonstrates a place where there is a missing rule. There is not a clearly held and understood rule about who can and cannot access the child's information known to parents.

Design Implications:

- Support ambiguity over who accesses a child's information

Parent-P00 Interview Transcript:

*Laurian: who do you think can access your child's file?*

*Parent1: I'm sure, having thought about it, that I can access it but I've never asked and I'm not even sure what we be contained in there that I'd want to see other than accident reports and I'm sure the administrator can but I don't know beyond that..*

*Laurian: So you think the administrator can access your child's file, do you think the teachers can access your child's file?*

*Parent1: well I'm sitting here wondering if - I'm sure that they can but I don't know - I'm trying to think of a reason for that they shouldn't but I can't come up with one*

*Laurian: What about the owners?*

*Parent1: I would think that the owners could and I actually like the owners but they just have trouble getting a good person for there so... I would think that if they own the business they ought to have access to them*

...

*Laurian: Can you think of anybody you wouldn't want to have access?*

*Parent1: I don't have any situations... I guess just generally I wouldn't want it publicized... like <child>'s file is <child>'s file... I'm not sure I would want it open - I'm not sure I have a good reason for not wanting it open other than it's private... and really I don't know what's in that file beyond the accident forms*

*Laurian: Do you ever wonder about?==*

*Parent1: Now I do!*

*Laurian: Now you do! I'm glad I did that for you*

Parent-P02 Interview Transcript:

*Edgardo: Sure. If there is. Who do you think can access the information that you've given at the childcare?*

*P2: I guess the officers in the day care the main teacher the director*

*Laurian: Who else do you think can access it?*

*P2: I guess some of the confidential information even the teachers cannot get just the officers, the officials the directors.*

*Laurian: Can you give a sample piece of information that you think the teachers wouldn't be able to access.*

*P2: Maybe they can because I seen in the front office of <Child-P01> they have a big file cabinets. Last time I was handing them the doctor's signature immunization form they just put it in each folder so i guess for us every time we went in so if their teachers want to get it i have no idea what they do*

Parent-P03 Interview Transcript:

*P3: You know I'm probably guessing that the director or enrollment person probably has access to that. I would probably say that if they have someone who does their financial they have access to that. But as far as if I could give you an exact list, no.*

*Edgardo: And so do you think that anyone else can access this information apart from these other three people?*

*P3: Teachers too. I forgot those. They could probably be added to the list. I hope not. But, I don't know that.*

Parent-P04 Interview Transcript:

*Edgardo: Okay. Do you think anyone who has access or is it just those people*

*P4: No idea. Never thought about it.*

Parent-P08 Interview Transcript:

*Edgardo: Gotcha. You answered my question. Uh. Now we are kind of getting to the data access side of things. Um. Who are you aware of who can access your child's information*

*P8: No I am not*

*Edgardo: Okay. And could you guess of who you think has access*

*P8: I would think that the owner could access and the office manager um and you know I don't know if they have assistants or people who may help in the afternoon who parents because there are a lot of parents who are coming in the afternoon to pick up their children so I don't know if they have other folks but I would say that I would feel comfortable with just the office manager and the owner there having access*

Parent-P09 Interview Transcript:

*P9: I think uh the the director or the social director I don't know if the teacher will actually go to check the uh enrolled information*

*Edgardo: Um so do you think that the teacher can put things in your child's file*

*P9: Yeah I think so I also think that the administrative staff know I mean some some sheets they ask to know about my son yeah*

Parent-P14 Interview Transcript:

*Zalia: Do you know who has access to your child's information?*

*Participant14: I am assuming...we have two owners and a director and assistant director. And the assistant director is also a teacher in one of the classrooms.*

*Zalia: So... you think they are.*

*Participant14: Yeah, I think these four people.*

*Zalia: Anyone else?*

*Participant14: I assume no.*

Parent-P15 Interview Transcript:

*Zalia: Do you know who has access to your child's information? Is it only owners and site workers?*

*Participant15: Right. I am really not sure.*

Parent-P17 Interview Transcript:

*Zalia: Who do you think can access, may be not the outsiders, I mean the person who are there?*

*Participant17: Who are there? I assume the secretary and the manager, like the owner, manager-owner, I assume just that. Not even the teachers. Not the teachers.*

*Zalia: Not the teachers?*

*Participant17: Yeah not even the teachers.*

Parent-P18 Interview Transcript:

*Zalia: So, the child's information, I mean your child's information, they put it in files or something. Do you know who have access to your child's information in report or..?*

*Participant18: I don't know. I presume that the administrators and teachers. I presume if there is an accident then doctors would have access to it. My daycare is owned by people who actually don't work there. The business is owned by people who live in Arizona somewhere. I presume they have access to it, if they care to and beyond that I presume that people don't look at it but I doubt it. I don't know.*

*Zalia: And do you know if there is any hierarchy or what is your thought about that? May be your child's teacher do not need their health information similarly may be your child's doctor does not need what he likes or not likes.*

*Participant18: I actually wondered if the teachers actually read those because a lot of those forms you know we are saying this is my child's disposition and these are the things at he is really good. I always presume that the teachers will take time to read that but I don't know. I don't know that anybody reads that. I think I am going and get to see what they do. I do presume that folks do tend to be more likely to read that information when the child is either new to the center or if they are younger to do. Because when I started my baby, two days after she started, the teachers talked to me about some of the things that I wrote down. So I know that they read it. With my son at age almost seven are they reading those things, I don't know. And also there is lots of turnovers you know lots of new teachers, new floaters, new temporary people coming in and out and so I don't presume they are reading those stuffs. We also have a new administrator in the past several months, has she read all those stuffs, I got it. So, I don't know what's going on.*

Parent-P20 Interview Transcript:

*Participant20: Is there anyone outsider like the people who aren't at the day care? Or...*

*Zalia: In general, may be if they are in daycare there are some teachers, there are some owners or some other person. So, do you know who have access or... and also if there are some outsiders are allowed to access or not?*

*Participant20: Well. <External-5> is run by the place in Christiansburg and I assume that any of their workers would have access to the records there. I don't know if that is computer kept or if it is actually paper kept. I know they have lot of papers every year. So, I assume that any of their workers would have access to that. As far as school information you know the teachers like parent volunteers, the principal... I mean I don't really know for sure but I think any of the people that work for their school would have access to their records. But I don't need for sure.*

### **9.83 Parents Lacking Confidence in Childcare Keeping Information Safe (Study1)**

Interview:

- Parent-P01
- Parent-P02
- Parent-P05
- Parent-P07
- Parent-P10
- Parent-P11
- Parent-P12
- Parent-P15
- Parent-P18

During their interview parents were asked about how they thought that their childcare was managing their information. When asking this question it was unearthed that a few parents believed that their childcare was capable of managing their child's care, but not managing the care of the child's information. Parents felt that the childcare staff were good at taking care of children, but in terms of understanding the spectrum of different ways that private information could be mismanaged the parents felt that the childcares were inadequate.

This breakdown reflects a general breakdown in the trust level between the parallel activities of managing the care of the child with managing the care of the child's information. Parent-P03 even said, "I guess you always just assume that you are trusting them with that information and your child." Parents do not feel that one activity has the correct tools, and therefore the objective is not as easily accomplished.

Design Implications:

- Support parents and childcares knowing how information is being managed in childcares.

Parent-P01 Interview Transcript:

*P1: I do want to clarify. You asked about my confidence in keeping my child's information secure. I want to clarify that I don't think that they would willfully disseminate any information. I just, knowing people, and knowing that kind of stuff, I am not at all confident that someone couldn't break in or access that information illegally.*

Parent-P02 Interview Transcript:

*P2: Yeah. I think that if someone really wants to get that information they can get it. It is better if some people have such intention. If they want to steal it, it is not that hard*

*Laurian: Can you give an example?*

*P2: I think their folders in the filing cabinet if someone can see the schedule they can sneak in and get something or if some people the insider they work inside it is easy for them*

Parent-P05 Interview Transcript:

*Edgardo: Okay. And how much do you actually trust your childcare with that information that you've given them*

*P5: Well you know that is a good question. Um. you know you just trust that they are following the law the HIPPA laws and not sending your information across without some kind of security and I am pretty confident that that is what they do you know that as soon as I fill some paperwork out she takes it straight to the back it is a different office not the front desk and they have this locked cabinet that they put this information which is also a HIPPA requirement and um so hopefully you just have to trust*

*Edgardo: So you just kind of trust them out of blind faith*

*P5: Well yeah I guess pretty much.*

Parent-P07 Interview Transcript:

*Edgardo: Great. Great. How much do you trust your childcare with the information that you've given them*

*P7: 80%*

*Edgardo: Okay. And why do you give it 80%*

*P7: There are always those people who let things fall*

*Edgardo: So you think that the directors will let stuff out*

*P7: Well She hands the office over to other people to work and a parent comes in and sees it on a desk I believe when you are dealing with that many kids it is going to be kind of hard to uh keep everything locked down from all eyes*

Parent-P10 Interview Transcript:

*Edgardo: And uh how much do you trust the childcare with the packet of information that they have on you guys*

*P10: Huh. You know unfortunately I don't think that they think whatever information we've given them uh as uh you know it is not like a business that is I don't know that they have procedures in place if they do I am unaware of them I would hope that they do but I don't know that they have procedures in place for them.*

*Edgardo: So you kind of trust them*

*P10: I would say that uh I don't think that they going out and trying to sell my information to make money but I think that there would be an*

*opportunity uh inadvertently for that information to get out. So you know I do trust them to not go out and do it maliciously*

Parent-P11 Interview Transcript:

*Laurian: How you feel the information is made secure out these papers?*

*Participant11: Well I guess, as far as I fell about my perception is that it is more secure at <Child-P06>. Just a couple of places are more secure. I don't know where my information is kept but I just feel like there is someone keeping an eye on the front desk at <Child-P06> and there was not always at <Child-P09>. So I don't know that someone could have riffled through the information at <Child-P09> but everything the desk and everything was much more access able there.*

Parent-P12 Interview Transcript:

*Zalia: So, How much do you trust your childcare with your child's information regarding the accessing part?*

*Participant12: This place now, if it is on skill from 1 to 10, I would give them like 3 for trusting them. The first place in Atlanta, I would give them may be a 7, and the one in Roanoke was very sort of high quality more than I would like to keep him in. I would give them 8 and so. You can't even get into the door, unless they buzzed you in and they knew who you are and that sort of thing.*

...

*Laurian: You know like I have an issue and he is like four miles away.*

*Participant12: I wouldn't even say so much trust but it is almost like necessity and I trust my family. I guess that what I could say. My mom isn't in good enough health to keep him. Because that would be my ideal situation. But, I trust them because out of my immediate family all of them are there with in five to ten minute drive from him. So, I don't necessarily trust them so much as I trust to be able to get in contact with my family and get them to help or get them to go get him or whatever the need be if I must be out here as it were. Ideally it would be one I wouldn't have the commute, I would rather be there or we would both be here and he would be five minutes away so that I could see him at lunch and things of that sort so.*

Parent-P15 Interview Transcript:

*Zalia: How much do you trust your childcare regarding your child information?*

*Participant15: Like percentage?*

*Zalia: umm Yeah.*

*Participant15: I would say probably 90%. Not that you can fully trust anybody but I feel comfortable with the people that are in charge. But still there is always gonna be that motherly instinct that you will not completely trust anyone other than yourself to take care of your children.*

*Zalia: So, was there something that made you feel.. I mean at least 90% trusted?*

*Participant15: Well, I can tell you what made 10% untrusting is that some of the site workers are in high schools or just graduated from high school. And so, most of them never really you know had children of their own and so I am little uneasy about if they know what to do about certain situations. But we did not have any negative feelings.*

*Zalia: But you are conscious about it.*

*Participant15: You are right.*

*Zalia: And you want to know what actually is happening there?*

*Participant15: Right.*

*Zalia: because you don't have any daily report.*

*Participant15: Right.*

#### Parent-P18 Interview Transcript:

*Participant18: I have no idea. I have not thought about. I just presume that there are files and there is a literally paper file for my child which honestly does not bother me as much of the idea of information being on computer or such. You know what I mean. I just do not trust that there is any sort of sophisticated security system whether it is on paper or electronically to protect the information. But I actually never asked where these information go. I just sort of entrusted it although I feel like I haven't put their social security numbers on there.*

...

*Zalia: yes. It is. So, how much you trust your childcare about your child's information?*

*Participant18: I trust them. I do. I believe they collect and use the information in good faith; I don't presume that there would be a violation of confidentiality that was deliberate. My concerns are more around... you know they daycare workers are not security officers what they do they really know about securing information and if it is information that is on the computer they are not computer scientists. I don't think that they can afford to hire a computer scientist to make sure that... you know special security programs on their computers. So in terms of good face I trust them completely. In terms of the real world and the fact. You know identity theft is a growing problem. So my level of trust... I don't trust anybody at that level. The fact that I know that I can be stolen from my bank or you know from my clothing place, I just order place a new pant from online. So do I trust them as individuals? Sure I do. Do I trust globally then something that go along? No.*

### **9.84 Children's Pictures on Facebook (Study 1)**

Interview:

- Parent-P12
- Parent-P13

There was only one instance where a parent felt that their privacy was not respected. In this case it was when a teacher posted pictures of children in the classroom on her Facebook account. A parent had discovered the pictures when she became “friends” with the teacher on Facebook. The issue was resolved by having the pictures removed from the account along with changing the policy about posting pictures.

In this example the breakdown occurred because of the lack of explicit rule surrounding how pictures of children should be managed. With the lack of this rule, the teacher desired to post pictures of her work on her account, and the teacher thought she was following regulations surrounding the children’s privacy.

Parent-P12 Interview Transcript:

*Participant13: The only other thing that I think would be important for us is what happens to your childrens’ photograph. This did not happen to me but happed to a friend of mine. She ended up being on Facebook and became friends with some of the teachers on Facebook. And the teachers were posting the pictures of their children on the Facebook. So, she then called the administrators and they got them pull off of Facebook. But I think that, I think pictures of your children to me actually is important for me and Rainbow Riders have me signed a release around the pictures that is it okay for your child to be photographs or is that okay for certain things for photographs.*

Parent-P13 Interview Transcript:

*Zalia: So, how much do you trust your childcare with your child’s information?*

*Participant14: ummm.*

*Zalia: And their personal information about you too, like your address or something.*

*Participant14: Right. I trust the record a lot right now. Just recently we had a facebook issue.*

*Zalia: What is that?*

*Participant: Two or three of the teachers had friended me on facebook. An a week later in looking at their facebook I noticed that they had pictures of the children playing in that I daycare on their facebook. So, that afternoon, I called the daycare and told the director. It was like three o’clock in the afternoon. Then when I got there to pick them up the owner was there. So she pulled me aside and apologized and said that it would get fixed. And they brought all the securities, teachers into the office and watched them take the picture down off from the internet before they left that day. So, they are definitely on it as far as fixing the problem and that’s the feeling of nervousness that I have. You know just like very personal pictures are up.*

*Zalia: Did they give your children’s picture in facebook any time after that?*

*Participant14: No. Well I went to their facebook pages to check to make sure if they are gone and they are gone.*

*Zalia: And that did not happen later?*

*Participant14: They unfriended me. So, I have no access to the picture any more. So, I am assuming. I don't know.*

*Zalia: But was there any other parents who still have access to the facebook account?*

*Participant14: I don't know. And it was only three. I had access to only three teachers and you know there are twelve teachers maybe at the school. So, that's why I went to the directors versus just going to specifically to make sure there is a widespread statement made.*

*Zalia: Yeah that was great that you talked directly to the director but the thing is that you could not check after that whether they still doing these type of things.*

*Participant14: Right, exactly, yeah.*

## **10 Appendix B, List of Informed Consents**

### ***10.1 Informed Consent for Interviewing Childcare Center Directors & Parents***

Investigators: Steve Harrison, Dr. Dennis G. Kafura, Laurian Vega, Tom DeHart, Edgardo Vega, Zalia Shams

#### **Purpose of this Research**

The purpose of this research is to start investigating how personal information is accessed, documented, and stored in medical-like settings. The goal is to develop an understanding from the interviews that will better inform the design and study of personal health records.

#### **Procedures**

At the start of the interview we will ask for demographic information about you and the childcare center you work for or are associated with for our record keeping purposes. Next, we will ask questions to start you thinking about what are the kinds of information that is stored in the childcare center, who can access that information, how is that information accessed and is there an audit trail, and how is that information documented. We will then work to fill in a table that diagrams all of the people, information, and access rights. This interview can be interrupted for job related tasks. Without interruption we anticipate this interview to take between 30 and 45 minutes. At the end of the interview you will be thanked for your time.

#### **Risks**

The only known risk in this study is legal. We do not wish to see any information that is confidential or illegal to share. However, all information and audio will be stored in a password-protected computer. Files will only be named with your participant number that is written at the top right of this form.

**Benefits**

The long term benefits of this study is that the information you provide will give us insights into how personal information is managed in medical-like situation. This will guide us in the design of electronic personal information management. This will help reduce time, cost, and paperwork in the medical and childcare center settings.

However, no promise or guarantee of benefits has been made to encourage you to participate in this research. If at a later date, if you are interested in the results of this study, you can contact the researches listed below for a summary.

**Extent of Anonymity and Confidentiality**

At the beginning of the study you will be assigned a random participant number to assure your confidentiality. You can see this number at the top of the informed consent. There are a few places you identification will be stored. One is on our copy of this form. The second will be in a digital file that associates your name with your participant number. The third is in the audio recording of the interview. The last is on notes that we may take during the interview. These file will all digitized and secured under a password, and the informed consents will be stored in a locked file cabinet under the protection of the investigators. At no time will the researchers release identifying information to anyone other than individuals working on the project without your written consent.

During the interview we will be taking hand notes and filling out a table as well as taking an audio file of what you are saying. These recordings and notes will be stored on an external drive and also locked in a file cabinet of the experimenters. All data will be destroyed within 5 years of the experiment by either shredding the documents or whipping the hard drive.

It is possible that the Institutional Review Board (IRB) may view this study's collected data for auditing purposes. The IRB is responsible for the oversight of the protection of human subjects involved in research.

Unless the participant reveals information regarding abuse to him/herself and/or others, this confidentiality will be maintained under all circumstances

**Compensation**

You will be compensated \$10.00 for participating in this study.

**Freedom to Withdraw**

You are free to withdraw from a study at any time without penalty. You are free not to answer any questions or respond to experimental situation that you choose without penalty.

There may be circumstances under which the investigator may determine that you should not continue as a subject. You will be thanked for you time.

**Subject's Responsibilities**

I voluntarily agree to participate in this study. I have the following responsibilities: to let the experimenter know if I am feeling overly frustrated and need to take a break; to let the experimenter know that I need to leave the study.

**Subject's Permission**

I have read the Consent Form and conditions of this project. I have had all of my questions answered. I hereby acknowledge the above and give my voluntary consent:

\_\_\_\_\_ Date: \_\_\_\_\_

Subject Signature

Should I have any pertinent questions about this research or its conduct, and research subjects' right, and whom to contact in the event of a research-related injury to the subject, I may contact:

Laurian C. Vega, Steve Harrison (Faculty Advisor), Dr. Dennis Kafura (Faculty Advisor),  
Tom Dehart, Edgardo Vega, Zalia Shams  
Computer Science Department  
2202 Kraft Drive  
Blacksburg, VA. 24060  
{lhobby, srh, kafura}@cs.vt.edu, tdehart@gmail.com  
Phone: 540-231-7409

Dr. Ryder  
Department Head, Computer Science Department  
2202 Kraft Drive  
Blacksburg, VA 24060  
Ryder@cs.vt.edu  
Phone: 540.231.8452

David M. Moore  
Chair, Virginia Tech Institutional Review  
Board for the Protection of Human Subjects  
Office of Research Compliance  
2000 Kraft Drive, Suite 2000 (0497)  
Blacksburg, VA. 24060  
540.231.4991  
MooreD@vt.edu

## ***10.2 Informed Consent for Interviewing Physician's Office Directors***

Investigators: Steve Harrison, Dr. Dennis G. Kafura, Dr. Francis Quek, Laurian Vega, Laura Agnich

### **Purpose of this Research**

The purpose of this research is to start investigating how personal information is accessed, documented, and stored in medical settings. The goal is to develop an understanding from the interviews that will better inform the design and study of personal health records.

### **Procedures**

At the start of the interview we will ask for demographic information about you and the physician's office you work for or are associated with for our record keeping purposes. Next, we will ask questions to start you thinking about the kinds of information that is stored in the physician's office who can access that information, how is that information accessed, any audit trail, and how is that information documented. We will then work to fill in a table that diagrams all of the people, information, and access rights. This interview can be interrupted for job related tasks. Without interruption we anticipate this interview to take between 30 and 45 minutes. At the end of the interview you will be thanked for your time.

### **Risks**

The only known risk in this study is legal. We do not wish to see any information that is confidential or illegal to share. However, all information and audio will be stored in a password-protected computer. Files will only be named with your participant number that is written at the top right of this form.

### **Benefits**

The long term benefits of this study is that the information you provide will give us insights into how personal information is managed in medical situations. This will guide us in the design of electronic personal information management for personal health records. It will help reduce time, cost, and paperwork in the medical setting.

However, no promise or guarantee of benefits has been made to encourage you to participate in this research. If at a later date, if you are interested in the results of this study, you can contact the researches listed below for a summary

### **Extent of Anonymity and Confidentiality**

At the beginning of the study you will be assigned a random participant number to assure your confidentiality. You can see this number at the top of the informed consent. There are a few places you identification will be stored. One is on our copy of this form. The second will be in a digital file that associates your name with your participant number. The third is in the audio recording of the interview. The last is on notes that we may take during the interview. These files will all be digitized and secured under a password, and

the informed consents will be stored in a locked file cabinet under the protection of the investigators. At no time will the researchers release identifying information to anyone other than individuals working on the project without your written consent.

During the interview we will be taking hand written notes and filling out a table as well as taking an audio file of what you are saying. These recordings and notes will be stored on an external drive and also locked in a file cabinet of the experimenters. All data will be destroyed within 5 years of the experiment by either shredding the documents or whipping the hard drive.

It is possible that the Institutional Review Board (IRB) may view this study's collected data for auditing purposes. The IRB is responsible for the oversight of the protection of human subjects involved in research.

Unless the participant reveals information regarding abuse to him/herself and/or others, this confidentiality will be maintained under all circumstances.

### **Compensation**

There is no formal compensation for participating in this study.

### **Freedom to Withdraw**

You are free to withdraw from a study at any time without penalty. You are free not to answer any questions or respond to experimental situation that you choose without penalty.

There may be circumstances under which the investigator may determine that you should not continue as a subject. You will be thanked for your time.

### **Subject's Responsibilities**

I voluntarily agree to participate in this study. I have the following responsibilities: to let the experimenter know if I am feeling overly frustrated and need to take a break; to let the experimenter know that I need to leave the study.

### **Subject's Permission**

I have read the Consent Form and conditions of this project. I have had all of my questions answered. I hereby acknowledge the above and give my voluntary consent:

\_\_\_\_\_ Date: \_\_\_\_\_  
Subject Signature

Should I have any pertinent questions about this research or its conduct, and research subjects' right, and whom to contact in the event of a research-related injury to the subject, I may contact:

Laurian C. Vega, Laura Agnich, Steve Harrison (Faculty Advisor), Dr. Dennis Kafura  
(Faculty Advisor), Dr. Francis Quek  
Computer Science Department  
2202 Kraft Drive  
Blacksburg, VA. 24060  
{lhobby, srh, kafura}@cs.vt.edu, tdehart@gmail.com  
Phone: 540-231-7409

Dr. Ryder  
Department Head, Computer Science Department  
2202 Kraft Drive  
Blacksburg, VA 24060  
Ryder@cs.vt.edu  
Phone: 540.231.8452

David M. Moore  
Chair, Virginia Tech Institutional Review  
Board for the Protection of Human Subjects  
Office of Research Compliance  
2000 Kraft Drive, Suite 2000 (0497)  
Blacksburg, VA. 24060  
540.231.4991  
MooreD@vt.edu

### ***10.3 Informed Consent for Observations in Childcare Centers***

Investigators: Steve Harrison, Dr. Dennis G. Kafura, Laurian Vega, Stacy Branham, Monika Akbar

#### **Purpose of this Research**

The purpose of this research is to start investigating how personal information is accessed, documented, and stored in medical-like settings. The goal is to develop an understanding from the interviews that will better inform the design and study of personal health records.

#### **Procedures**

This is an observation study. We hope to ‘shadow’ you and watch you in your regular every day job for approximately 3 hours of time. During this time we will try not to be overly obtrusive. When there are any calm moments we may ask a couple of questions to clarify something we have seen or heard for our notes. Otherwise, we will be silent. At the end of the interview you will be thanked for your time.

#### **Risks**

The only known risk in this study is legal. We do not wish to see any information that is confidential or illegal to share. However, all information and audio will be stored in a password-protected computer. Files will only be named with your participant number that is written at the top right of this form.

#### **Benefits**

The long term benefits of this study is that the information you provide will give us insights into how personal information is managed in medical-like situation. This will guide us in the design of electronic personal information management. This will help reduce time, cost, and paperwork in the medical and childcare center settings.

However, no promise or guarantee of benefits has been made to encourage you to participate in this research. If at a later date, if you are interested in the results of this study, you can contact the researchers listed below for a summary.

#### **Extent of Anonymity and Confidentiality**

At the beginning of the study you will be assigned a random participant number to assure your confidentiality. You can see this number at the top of the informed consent. There are a few places your identification will be stored. One is on our copy of this form. The second will be in a digital file that associates your name with your participant number. The third is in the audio recording of the interview. The last is on notes that we may take during the interview. These files will all be digitized and secured under a password, and the informed consents will be stored in a locked file cabinet under the protection of the investigators. At no time will the researchers release identifying information to anyone other than individuals working on the project without your written consent.

During the observation we will be taking hand notes as well as taking an audio file of what you are saying and doing. These recordings and notes will be stored on an external drive and also locked in a file cabinet of the experimenters. All data will be destroyed within 5 years of the experiment by either shredding the documents or whipping the hard drive.

It is possible that the Institutional Review Board (IRB) may view this study's collected data for auditing purposes. The IRB is responsible for the oversight of the protection of human subjects involved in research.

Unless the participant reveals information regarding abuse to him/herself and/or others, this confidentiality will be maintained under all circumstances.

### **Compensation**

No monetary compensation will be provided for participation in this study.

### **Freedom to Withdraw**

You are free to withdraw from a study at any time without penalty. You are free not to answer any questions or respond to experimental situation that you choose without penalty.

There may be circumstances under which the investigator may determine that you should not continue as a subject. You will be thanked for your time.

### **Subject's Responsibilities**

I voluntarily agree to participate in this study. I have the following responsibilities: to let the experimenter know if I am feeling overly frustrated and need to take a break; to let the experimenter know that I need to leave the study.

### **Subject's Permission**

I have read the Consent Form and conditions of this project. I have had all of my questions answered. I hereby acknowledge the above and give my voluntary consent:

\_\_\_\_\_ Date: \_\_\_\_\_  
Subject Signature

Should I have any pertinent questions about this research or its conduct, and research subjects' right, and whom to contact in the event of a research-related injury to the subject, I may contact:

Laurian C. Vega, Steve Harrison (Faculty Advisor), Dr. Dennis Kafura (Faculty Advisor),  
Stacy Branham, Monika Akbar

Computer Science Department  
2202 Kraft Drive  
Blacksburg, VA. 24060  
{lhobby, srh, kafura}@cs.vt.edu, tdehart@gmail.com  
Phone: 540-231-7409

Dr. Ryder  
Department Head, Computer Science Department  
2202 Kraft Drive  
Blacksburg, VA 24060  
Ryder@cs.vt.edu  
Phone: 540.231.8452

David M. Moore  
Chair, Virginia Tech Institutional Review  
Board for the Protection of Human Subjects  
Office of Research Compliance  
2000 Kraft Drive, Suite 2000 (0497)  
Blacksburg, VA. 24060  
540.231.4991  
MooreD@vt.edu

## ***10.4 Informed Consent for Observations of Physician's Office Directors***

Investigators: Steve Harrison, Dr. Dennis G. Kafura, Dr. Francis Quek, Laurian Vega, Tom DeHart, Aubrey Baker.

### **Purpose of this Research**

The purpose of this research is to start investigating how personal information is accessed, documented, and stored in medical settings. The goal is to develop an understanding from the interviews that will better inform the design and study of personal health records.

### **Procedures**

This is an observation study. We hope to 'shadow' you and watch you in your regular every day job for approximately 3 hours of time. During this time we will try not to be overly obtrusive. When there are any calm moments we may ask a couple of questions to clarify something we have seen or heard for our notes. Otherwise, we will be silent. At the end of the observation you will be thanked for your time.

Please note that the Medical Director at your practice has granted us permission to conduct this study; however, the director does not endorse this research nor will he or she be provided raw research data.

### **Risks**

The only known risk in this study is legal. We do not wish to see any information that is confidential or illegal to share. However, all information will be stored on an encrypted external hard drive locked in a file cabinet. Files will only be named with your participant number that is written at the top right of this form.

### **Benefits**

The long term benefit of this study is that the information you provide will give us insights into how personal information is managed in medical situations. This will guide us in the design of electronic personal information management for personal health records. It will help reduce time, cost, and paperwork in the medical setting.

However, no promise or guarantee of benefits has been made to encourage you to participate in this research. If at a later date, if you are interested in the results of this study, you can contact the researchers listed below for a summary

### **Extent of Anonymity and Confidentiality**

At the beginning of the study you will be assigned a random participant number to assure your confidentiality. You can see this number at the top of the informed consent. There are a few places your identification will be stored. One is on our copy of this form. The second will be in a digital file that associates your name with your participant number. The last is on notes that we may take during the interview. These files will all be digitized and secured under a password, and the informed consents will be stored in a locked file cabinet under the protection of the investigators. At no time will the researchers release

identifying information to anyone other than individuals working on the project without your written consent.

During the observation we will be taking hand notes of what you are saying and doing. These notes will be stored on an external drive and also locked in a file cabinet of the experimenters. All data will be destroyed within 5 years of the experiment by either shredding the documents or whipping the hard drive.

It is possible that the Institutional Review Board (IRB) may view this study's collected data for auditing purposes. The IRB is responsible for the oversight of the protection of human subjects involved in research.

Unless the participant reveals information regarding abuse to him/herself and/or others, this confidentiality will be maintained under all circumstances.

**Compensation**

No monetary compensation will be provided for participation in this study.

**Freedom to Withdraw**

You are free to withdraw from the study at any time without penalty. You are free not to answer any questions or respond to experimental situation that you choose without penalty.

There may be circumstances under which the investigator may determine that you should not continue as a subject. You will be thanked for you time.

**Subject's Responsibilities**

I voluntarily agree to participate in this study. I have the following responsibilities: to let the experimenter know if I am feeling overly frustrated and need to take a break; to let the experimenter know that I need to leave the study.

**Subject's Permission**

I have read the Consent Form and conditions of this project. I have had all of my questions answered. I hereby acknowledge the above and give my voluntary consent:

\_\_\_\_\_ Date: \_\_\_\_\_  
Subject Signature

Should I have any pertinent questions about this research or its conduct, and research subjects' right, and whom to contact in the event of a research-related injury to the subject, I may contact:

Laurian C. Vega, Tom DeHart, Steve Harrison (Faculty Advisor), Dr. Dennis Kafura  
(Faculty Advisor), Dr. Francis Quek  
Computer Science Department  
2202 Kraft Drive  
Blacksburg, VA. 24060  
{lhobby, srh, kafura}@cs.vt.edu, tdehart@vt.edu  
Phone: 540-231-7409

Dr. Ryder  
Department Head, Computer Science Department  
2202 Kraft Drive  
Blacksburg, VA 24060  
Ryder@cs.vt.edu  
Phone: 540.231.8452

David M. Moore  
Chair, Virginia Tech Institutional Review  
Board for the Protection of Human Subjects  
Office of Research Compliance  
2000 Kraft Drive, Suite 2000 (0497)  
Blacksburg, VA. 24060  
540.231.4991  
MooreD@vt.edu

## 11 Appendix C, List of Instruments

### *11.1 Interview Protocol for Interviewing Childcare Center Directors*

#### **Section 1: Demographic and Background Information**

Goal: To collect background information about the person and childcare center.

Name: \_\_\_\_\_

Gender: M/F

Are you a parent? Yes/No

If so, how old is/are your child/children: \_\_\_\_\_

Childcare Facility: \_\_\_\_\_

Title: \_\_\_\_\_

Number of children currently enrolled at this location: \_\_\_\_\_

Number of children you personally oversee: \_\_\_\_\_

Number of people whom you work with at this location: \_\_\_\_\_

Age range of children whom you're responsible for: \_\_\_\_\_

How long have you been working at this particular location: \_\_\_\_\_

How long have you been working in Childcare Services: \_\_\_\_\_

#### **Section 2: Information Security**

Goal: To look at the various dimensions of information that is documented, stored, and communicated. This section is to get the participant thinking about information they interact with and collect.

Time and Variety:

What is the information that you handle as part of your duties at this facility daily?  
Weekly? Monthly? What is routine and what is event-driven?

Types:

What are some of the types of information you interact with and how is it handled?  
Health? Immunization? Age? Behavior? Incidents? (e.g. illness, physical altercations between children, etc) Parents?

Do you or your facility have general policies about who can access information in your facility? How is it communicated to staff? To parents? To oversight agencies? Is there a situation that illustrates how this works?

How is access to information about children or other people managed?

Where are files stored? (Take picture)

How is information exchanged with: People who work here? Staff and individual parents? Groups of parents? Government and accreditation agencies?

Has your access to information changed? For instance, when you started working here, were you only allowed to access a minimal amount of information?

If applicable: What affect does access to the information of other children on your behavior or practices as a parent?

Maybe: Information Verification

What information verification procedures are followed? For instance, do you verify the child's or parent's social security number? What information does your childcare center provide to prove that they are certified? Maybe: When someone joins your childcare center, what precautions are taken?

### **Section 3: Interfaces for information**

Goal: To itemize all the stakeholders in information access and to understand how information and documented information flows.

See attached table~ Interview Form: Field Study of In-use Information Security and Interfaces within Childcare Center

### **Section 4: Web Camera**

Goal: The goal of this section is to probe how security is managed and access is granted.

Do you use web cameras in your Day Care? If yes: Who runs the web camera access system?

Maybe, if 3rd party: Do you have a copy of the contract? What made you pick this company?

What privacy policies are there? Who enforces them? Can I see what you can see through the web camera system? How is this view different or similar to what others can see? Who can access the system? What is the procedure for others to access the web camera system? How do you know when someone has accessed the system? What would happen or what has happened when there is suspicious activity in the web camera system? Is what is seen through the web-cameras ever recorded? What happens with those recordings? Who can access those recordings?

### Interview Form: Field Study of In-use Information Security and Interfaces within Childcare

Person	Different ways to communicate		Information they provide		Information they can access		Information kept on them	
	ex: email, phone, portal		ex: forms					
	Often	Method	Often	Method	Often	Method	Often	Method
Parent								
Child								
Owner								
Auditor								
Doctor								
Care Provider								
Administrator								

Person	Different ways to communicate		Information they provide		Information they can access		Information kept on them	
	ex: email, phone, portal		ex: forms					
	Often	Method	Often	Method	Often	Method	Often	Method
3rd Party Companies								

## ***11.2 Interview Protocol for Interviewing Physician's Office Directors***

### **Section 1: Demographic and Background Information**

Goal: To collect background information about the person and childcare center.

Name: \_\_\_\_\_

Gender: M/F

Health Care Facility: \_\_\_\_\_

Title: \_\_\_\_\_

Number of patients currently served at this location: \_\_\_\_\_

Number of patients you personally have contact with: \_\_\_\_\_

Number of people whom you work with at this location: \_\_\_\_\_

Number of doctors/physicians practicing at this location: \_\_\_\_\_

How long have you been working at this particular location: \_\_\_\_\_

How long have you been working in health care Services: \_\_\_\_\_

### **Section 2: Information Security**

Goal: To look at the various dimensions of information that is documented, stored, and communicated. This section is to get the participant thinking about information they interact with and collect.

Time and Variety: What is the information that you handle as part of your duties at this facility daily? Weekly? Monthly? What is routine and what is event-driven?

Types:

What are some of the types of information you interact with and how is it handled? Patient personal information (identity, SSN, contact,...)? Patient financial (payment method, account information...)? Patient medical record (history, illnesses, lab results...)? Patient medications (prescriptions...)? Insurance information? Schedule information (doctor daily schedule, patient scheduling...)? Referrals (to other specialists)? What is the kind of information you or others might hesitant to write down?

Do you or your facility have general policies about who can access information in your facility? How is it communicated to staff? To patients? To oversight agencies? Is there a situation that illustrates how this works?

Access

How many people have access to all the files? How is access to information about patients or other people managed?

Has there ever been a time when someone had access to information that they shouldn't? Or accessed information? What happened?

How long do you keep files stored? Where are files stored? (Take picture)

Has your access to information changed? For instance, when you started working here, were you only allowed to access a minimal amount of information?

Ask if time:

What affect does access to the information of other patients have on your behavior or practices as a patient? What information verification procedures are followed? For instance, do you verify the patient's social security number?

### **Section 3: Interfaces for information**

Goal: To itemize all the stakeholders in information access and to understand how information and documented information flows.

See attached table~ Interview Form: Field Study of In-use Information Security and Interfaces within health care

### **Section 4: Electronic Health Information Systems**

Goal: The goal of this section is to probe what information is maintained in electronic form, how security is managed and access is granted.

Do you use an electronic/computerized system for the maintenance of patient information? If yes: Who provides the electronic/computerized system?

What made you pick this company? What privacy policies are there? Who enforces them? What kinds of information are stored in the system? Who can access the system? What is the procedure for others to access the system? How do you know when someone has accessed the system? Who can add, modify, delete information to/from the system? Is the system only accessible on premises? Or, can it be accessed remotely? What would happen or what has happened when there is suspicious activity in the system?

### Interview Form: Field Study of In-use Information Security and Interfaces within Childcare

Person	Different ways to communicate		Information they provide		Information they can access		Information kept on them	
	ex: email, phone, portal		ex: forms					
	Often	Method	Often	Method	Often	Method	Often	Method
Parent								
Child								
Owner								
Auditor								
Doctor								
Care Provider								
Administrator								

Person	Different ways to communicate		Information they provide		Information they can access		Information kept on them	
	ex: email, phone, portal		ex: forms					
	Often	Method	Often	Method	Often	Method	Often	Method
3rd Party Companies								

### ***11.3 Interview Protocol for Interviewing Parents***

#### **Section 1: Demographic and Background Information**

Goal: To collect background information about the parent and their child or children.

Name: \_\_\_\_\_

Gender: M/F

Number of children in a childcare center: \_\_\_\_\_

Age(s) of child(ren): \_\_\_\_\_

Childcare Facility in which your children are enrolled in: \_\_\_\_\_

How long has/have your child/children been enrolled in a childcare program: \_\_\_\_\_

How long has/have your child been enrolled in the current childcare program: \_\_\_\_\_

#### **Section 2: Information Security**

Goal: To look at how information is shared between the childcare providers and to the parents that are enrolling their children in to such programs.

In order to enroll your child/children in to childcare center, what kind of information did you have to provide about yourself? What kind of information did you have to provide about your child/children? Forms? Immunizations?

Maybe: Was there any particular information that you had to provide to the childcare facility that you felt was unnecessary or sensitive? How was this information handled? Any differently?

What kind of information does the childcare facility provide to you about your child/children? (ex: daily reports, webcam feeds, etc) Daily? Weekly? Yearly?

Is there any sort of information that you might have gathered about other children that are enrolled in your child's/children's program (e.g. illnesses/conditions, behaviors )?

Are you aware of who can access your child's information? Who do you think can access your child's information?

Do you know that centers keep your files forever?

Who do you think is the owner the information in your child's file?

If you aren't comfortable with any policies do you feel you would be able to bring it up and have it be changed?

How much do you trust your childcare center with your child's information?

What reassurances have you been given that the information about your child has been protected? Do you know who has access to information about your child?

Maybe (intrusive): Has there ever been an incident between your child and another at the childcare center (e.g. physical altercations)?

If so, what kind of information was given to you about the incident (e.g. name of the other child, what exactly happened between the two children, etc)?

What are the different ways that you may be contacted by the childcare center (ex: phone, face-to-face, email, etc.)?

## *11.4 Letter of Introduction for Observations*



Department of Computer Science College of Engineering  
VIRGINIA POLYTECHNIC INSTITUTE

Steve Harrison  
121 VTKW II, 2202 Kraft Dr.  
Department of Computer Science – MC 0902  
Blacksburg VA 24060  
(540) 231 7783 sHarrison@vt.edu

June 2, 2010

This letter is to introduce members of the research team from the Department of Computer Science at Virginia Tech. Medical information systems are constantly and rapidly changing. Our research is intended to make those systems more responsive to the actual practices of medical offices. To do that, we are doing a study of small physicians' offices in the New River Valley area. The study entails having one or two of the members of the research group (Laurian Vega, Tom DeHart, Aubrey Baker, and myself) sit quietly and observe the flow of information in your practice.

This work builds on a study conducted last Fall which interviewed staff and physicians in small practices. From that, we have determined that there are many places information is coordinated between records and systems, and that there may be many special cases; we want to better understand them better by observing them directly.

As with our research will keep confidential anything we hear or see. We have strict guidelines to enforce this; they are spelled out in our Institutional Review Board Approval that you will be given a copy of. For example, we will not use any names of staff or patients; we will avoid looking at the contents of patient records; and we will not take pictures. Furthermore, we are acutely aware of issues of confidentiality since that is one of the key things we wish to study.

We greatly appreciate allowing us to do an observation of your practice. Ideally, we would observe for about two or three hours in order to see the ebb and flow of work, but any amount of time would be useful.

If you have any further questions, please do not hesitate to contact me.

Sincerely,

Steve Harrison  
Professor of practice, Computer Science and  
School of Visual Arts