Essays on Human Error in Electronic Health Records (EHR) Information Security

Wilmer Alvarado

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
Industrial and Systems Engineering

Konstantinos P. Triantis, Chair
Navid Ghaffarzadegan
Niyousha Hosseinichimeh
Roy C. Pettis

April 25, 2025
Arlington, Virginia

Keywords: Data Breaches, Electronic Health Records, Human Errors, HIPAA Penalties, Reason's Resiliency Model, Socio-Technical Systems

Essays on Human Error in Electronic Health Records (EHR) Information Security

Wilmer Alvarado

ABSTRACT

This dissertation presents a management framework designed to mitigate human error in information security, aiming to enhance the resilience of EHR systems to make them less attractive to cybercriminals. The framework enhances Reason's Resiliency Model by incorporating a socially oriented management approach based on socio-technical systems (STS) principles.

The information security literature presents evidence that human error is a significant contributor to cybersecurity incidents. Human error has increased the vulnerability of healthcare information, exposing it to persistent and increasingly sophisticated malicious cyberattacks that threaten the security and privacy of the American people. People continue to make mistakes and there is no single solution in cybersecurity that can reliably protect the system from vulnerabilities created by human-technology interface errors.

This dissertation focuses on the impact of error, as a consequence of the human-technology interface, in the information security of the healthcare sector. The research investigates: the role of STS factors for developing solutions aiming to enhance the resilience of EHR systems; how the location where data are breached influence the severity of data breaches impacting the security and privacy of patient records; how unintended consequences from EHR adoption impact the productivity performance of the states healthcare systems (DMUs); and, how the Health Insurance Portability and Accountability Act (HIPAA) monetary penalties influence compromised patient records.

This dissertation concludes that addressing EHR information security threats requires a fundamental shift in the healthcare sector's approach to data security. The research determines that integrating STS factors with Reason’s layered approach offers a

comprehensive management framework for mitigating human error challenges in healthcare information security. The findings show that network servers and emails are the two most common sites where healthcare data are breached capturing 95% of the 713 million compromised patient records since 2009. Empirical analysis indicates that despite privacy concerns resulting from data breaches, the overall productivity performance of the DMUs has improved over time. However, cybersecurity challenges continue to have an impact on the DMUs productivity performance. The findings also demonstrate that monetary penalties from HIPAA violations have not been effective in slowing down the number of compromised patient records in the sector.

Essays on Human Error in Electronic Health Records (EHR) Information Security

Wilmer Alvarado

GENERAL AUDIENCE ABSTRACT

President Biden's March 2023 National Cybersecurity Strategy outlines a path for achieving two significant shifts: the need for more capable cybersecurity-human actors to defend our systems and the need to make investments in long-term resilience capabilities. This dissertation addresses both paths. It presents a management framework to mitigate human error in information security, aiming to enhance the long term resilience of EHR systems and make them less attractive to cybercriminals. The framework builds on Reason's Resiliency Model to create a socially oriented management framework based on socio-technical systems (STS) principles.

The adoption of EHR technology has led to data breaches and compromised patient records as unintended consequences. While digital platforms in healthcare organizations are enabling the sector to provide better services to patients, they have also risen awareness about the increasing risk of healthcare system vulnerabilities to data breaches. Despite continuous investment in IT security, the sector continues to experience an increase in the volume of data breaches and their complexity, making them difficult to identify their location, prevent, and mitigate the severity to the security of patient records.

This dissertation focuses on the impact of error, as a consequence of the human-technology interface, in the information security of the healthcare sector. The significance of the problem is undisputable, as the present day healthcare has become the main victim of external and internal cybersecurity incidents. Data breach reports show that there has been a sharp increase in the number of compromised patient records in the last seven years. It is also observed that 84% of all data breaches are directly or indirectly caused by human error. Additionally, it is demonstrated that the

location where data are breached influence the severity of data breaches impacting the privacy of patient records.

The first hypothesis studies how the location where data are breached influences the severity of compromised patient records. To investigate this hypothesis, empirical data from the Department of Health and Human Services (DHHS) Office of Civil Rights (OCR) were analyzed to determine the most frequent locations where data are breached and their impact on patient records security.

The second hypothesis investigates the unintended consequences from EHR adoption, specifically how privacy concerns impact the productivity performance of the states healthcare systems (DMUs). A linear programming model using the Malmquist productivity index (MPI) was applied to assess productivity and technological improvements across three state clusters: high-capacity, mid-capacity, and low-capacity states. Historical data on compromised patient records from 2009 to 2022 were then used to formally test this hypothesis.

The third hypothesis evaluates whether monetary penalties influence the number of compromised patient records resulting from human error data breaches. To test this hypothesis, multiple regression analysis models were employed to assess the relationship between HIPPA violation penalties and the volume of patient records compromised in the sector.

This dissertation concludes that addressing EHR information security threats requires a fundamental shift in the healthcare sector's approach to data security. The research determines that integrating STS factors into Reason’s layered approach offers a comprehensive management framework for mitigating human error challenges in healthcare information security. The findings show that network servers and emails are the two most common sites where healthcare data are breached capturing 95% of the 713 million compromised patient records since 2009. Empirical analysis of the DMUs data indicates that despite privacy concerns resulting from data breaches, the overall

productivity performance of the healthcare sector has improved over time. However, cybersecurity challenges impact the DMUs productivity performance. The findings also demonstrate that monetary penalties from HIPAA violations as a result of human error have not been effective in slowing down the number of compromised patient records in the sector.

Dedication

I dedicate this dissertation to:

My wife, Nurys Alvarado, your love and unwavering support have been a constant source of inspiration and encouragement through the long hours of graduate school and throughout our life journey together. I am deeply grateful and truly fortunate to have your love in my life.

My children, Alexander and Sara, you are the brightest stars in my life. Thank you for being the most wonderful children a parent could ever hope for. You exemplify the true spirit of God's fourth commandment "honor your father and mother."

Acknowledgement

I want to offer my sincere gratitude to the many people who supported and assisted me throughout my doctoral journey and dissertation process. First and foremost, I would like to thank my advisor, Dr. Konstantinos Triantis, whose mentorship has been the most influential aspect during my tenure as a PhD student. Over the past four years, his extensive experience as a researcher and dissertation advisor, along with his insights to bridge research with practical application, has been invaluable to make my research a more meaningful contribution to the public. His guidance, insights, mentorship, and expertise on many aspects of my research, ranging from problem definition, performance measurement tools, and statistical analysis, combined with his sharp editing skills and detailed feedback, have significantly enhanced my skills as a modeler, statistician, writer, and researcher. I am very grateful for his support and commitment to my academic growth.

I want to thank my committee members, Dr. Navid Ghaffarzadegan for his valued feedback and insightful recommendations for improving the modeling aspects of my research. I had the opportunity to take a modeling course with Dr. Ghaffarzadegan, System Dynamics Modeling of STS, and learned immensely from his interactive and practical teaching approach. I also like to thank Dr. Niyousha Hosseinichimeh for her attention to details, valuable questions and feedback, and her thoughtful support that drove me to tailor the research scope and focus on the research purpose, saving me an immense amount of time to complete the degree, and improving the value and meaning of my dissertation and journal papers. Last but not least, I like to thank Dr. Roy Pettis for his valuable research recommendations and feedback, his friendship, and for volunteering his time from his busy daily schedule to be part of this dissertation committee. I enjoyed sharing my dissertation research papers, proposal, and plans with you, and this is a better dissertation because of all your help, valuable feedback, and recommendations.

I would also like to extend my gratitude to my System Performance Lab (SPL) research teammates, especially Dr. Konstantinos Triantis, Dr. Joseph Godfrey, Dr. Leon Sobrie,

and Dr. Maria Tomai, for kindly taking their time to reviewing the results of my dissertation performance measurement and statistical analyses in my dissertation. Their valuable feedback and recommendations have immensely improved the quality and impact of my research findings. I appreciate your candid insights, attention to details, and outstanding support. I cannot thank you enough for all your help.

The SPL research meetings are a great vehicle for sharing research information with other PhD colleagues and gaining the most needed feedback to improve everyone's dissertations. I cannot picture a better forum or academic environment to gain insights regarding the research process, modeling approaches, and analyses that enable us to progress in our dissertation journey. I sincerely thank you for your participation and to Dr. Triantis for leading the team. This is a very successful model that I plan to adopt in my future academic career.

Lastly, I would like to thank our department's Graduate Program Advisor, Hannah Parks, for the extraordinary support and assistance that she provides to our department's graduate students.

Table of Contents

List of Figures

List of Tables

Chapter 1.0: Introduction

1.1 Problem Context: Human Error in EHR Information Security

"We will make wider use of health information technology to help control costs and reduce dangerous medical errors," President George Bush, State of the Union, 2006.

The literature identifies the need for further research to investigate the impacts of Socio-Technical Systems (STS) factors on the reduction of human errors in information security. To address this gap, this dissertation develops a management framework incorporating STS factors that contribute to human errors, providing a conceptual understanding of their role in information security and identifying necessary improvements to reduce errors. This framework is designed to mitigate human error in information security, aiming to enhance the resilience of EHR systems to make them less attractive to cybercriminals.

The productivity performance of the U.S. healthcare system is a primary concern to government and industry leaders. Despite spending an estimated 18 percent of its 2023 gross domestic product in healthcare ($4.9 trillion or $14,570 per person), double the median of industrialized countries, the U.S. has one of the lowest performing healthcare system among all high-income countries. The U.S. is also not a leader in health information technology. "Given its collective wealth, technologic sophistication, and spending, the U.S. should lead, not lag, the world in its healthcare performance" (Harvard Business Review, 2024).

Keeping our nation competitive requires affordable and available healthcare. In 2004, President Bush launched an initiative to make EHR available to most Americans within the next 10 years. The EHR technology envisioned to help link together doctors, patients, and hospitals in seamless, digital environments, making it possible for patient records to be transferred quickly and accurately, and with all necessary privacy protections. Widespread use of digital information aims to help Americans receive high-quality medical care, save lives, prevent medical errors, and provide more affordable healthcare (Bush, 2006).

Digital healthcare services have paved the way for easier and more accessible treatment, thus making our lives far more comfortable. Advances in information and communication technology have helped the healthcare industry to replace paper-based systems with EHR to provide better and more cost-effective services to its customers. EHR enhance patient care, develop patient cooperation, enhance disease diagnosis, improve practice productivity, and make patient health information accessible all the time (Health IT, 2021). EHR are seen by the government and many experts in the field as the transformation technology that the sector needs to improve its performance and lower the cost of healthcare services to patients.

Spending in cybersecurity in the U.S. in the last decade exceeded $600 billion (Statista, 2024). And, it is expected to continue its ascending trend as cybersecurity has become the fastest growing crime in the U.S. The healthcare sector has been particularly vulnerable and targeted by cyberattacks because they store some of the most valuable information in the black market, including personal information, medical records, usernames, and passwords. Particularly, medical records are extremely valuable to thieves, selling for much more than stolen credit card numbers. Buyers can steal patients' identities, access financial accounts, and fraudulently obtain prescriptions. They can also contact patients directly with spam or threats. According to an IBM report (Ponemon Institute, 2024), the average cost of a healthcare data breach was estimated at $11 million in 2024.

The information security literature presents evidence that human error is a significant contributor to data breaches. People continue to make mistakes and there is no single solution in cybersecurity that can reliably protect the system from vulnerabilities created by human-technology interface errors. According to reports from Health Information Technology (IT) Security (Davis, 2021), cyberattacks against U.S. healthcare entities accounted for about 80% of all reported data breaches in 2020. Adoption of technology measures in the healthcare sector have contributed to increase awareness about system vulnerabilities to data breaches. But, despite continuous investment in IT to enhance information security systems, the sector continues to experience an increase

in the volume of data breaches and their complexity, making them difficult to identify their location, prevent, and mitigate their severity to the security and privacy of patient records.

The increasing trend in human error related data breaches highlights the need for a socio-technical systems (STS) thinking approach that goes beyond the technical aspects of the healthcare IT systems. This approach emphasizes the integration of organizational, human, and governmental factors to enhance system effectiveness and mitigate data breaches resulting from human-technology interactions. Human-technology interaction data breaches refer to security incidents in which sensitive or confidential healthcare information is exposed, compromised, or mishandled due to mistakes made by humans interacting with technology. These errors can occur at various levels within the healthcare organization and may involve multiple actions such as accidentally emailing sensitive information to the wrong recipient, misconfiguring the identity access security settings, lack of awareness, failure to follow established security protocols, or improperly implementing government policy.

An adverse consequence of the digitization of healthcare records has been the rapid ascent of cybersecurity incidents, primarily driven by human error related data breaches that are jeopardizing the privacy and security of protected health information (PHI). From the STS perspective, the application of the human factors engineering theory in the systems engineering field is concerned with the understanding of the interactions between humans and other elements of the system to mitigate the impact of human error on system performance. Highly technological systems, such as healthcare, are exceedingly becoming more complex (Qureshi, 2008). A primary characteristic of these systems is the high degree of human-technology collaboration required to deliver outcomes that couldn’t be possible in isolation. When patient records are compromised, EHR adoption, patient’s health safety, and information are put at risk.

Between 2009 and 2024, 6,594 healthcare data breaches were reported. These breaches resulted in the loss, theft, exposure, or impermissible disclosure of

741,340,196 patient healthcare records (DHHS OCR, 2024). Figure 1 presents the annual distribution of data breach incidents involving over 500 compromised records, along with the total number of compromised records by year. The figure illustrates that human error is the primary driver of data breaches, where out of the 6,594 incidents reported, 84% of these breaches and 95% of all compromised patient records were directly or indirectly caused by human error.

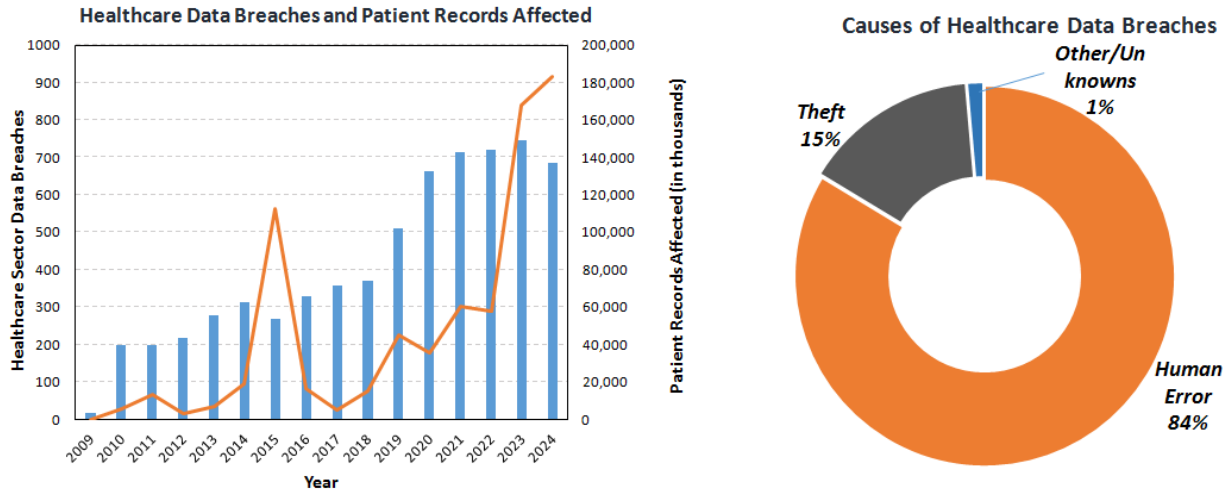


Figure 1: Historical Trend of Healthcare Data Breaches Based on 500 or More Records Compromised, Patient Records Affected, and Root Causes (HIPAA, 2024)

The interaction between humans and technology has an impact on economic productivity. Understanding and mitigating the impact of human-technology interface errors are essential components of effective economic production management. In information security, humans are often referred to as the weakest link in the security chain (Yan et al., 2018). Contrary to the general misconception of many information security practitioners, human error is the largest single cause of economic and productivity loss impacting information security in healthcare organizations (Zimmerman et al., 2019).

Healthcare information technologists have expressed concerns that, while human behavior and the resulting errors frequently lead to data breaches, and are a barrier to EHR adoption and information sharing (Gesulga et al., 2018), many existing security models have not adequately addressed the issue. Beyond focusing on the economic

impact of data breaches and consequences for patient services and healthcare providers' reputation, the role of human error as a barrier to EHR adoption and a threat to healthcare systems requires immediate attention.

The application of Reason's layered model as a framework for studying human error in EHR information security offers an opportunity to assess the effectiveness of individual security layers or combinations of multiple layers in mitigating successful healthcare data breaches. This model provides a visual representation of these safeguards and aligns with the systems thinking and STS approach presented in this dissertation.

Integrating the STS Management Framework with Reason's Resiliency Model aligns with the need for a holistic risk management approach, establishing a robust system of safeguards to enhance resilience against potential threats to EHR information security.

1.2 Theoretical Background: Reason's Resiliency Model

Reason's Accident Causation and the Human Factors Engineering theories share a common focus on understanding, prevention, and mitigating human errors in complex systems. Reason's theory, also known as the Swiss Cheese Model or Resiliency Model, is frequently used for explaining human error as the contributing factor to accidents (Reason, 2000).

Reason's Resiliency Model, Figure 2, describes how multiple layers of defense can fail and align in such a way that errors lead to accidents or incidents. The model is based on the principle of layered security to protect a system from accident causation. According to the model, causes of failures are on one side, accidents are on the opposite side, and in between are slices of Swiss cheese, or security layers. Swiss cheese is famous for its holes. When stacked, a bunch of random slices, the holes don't usually line up all the way through, which serve as security layers to avoid accident from happening (Perneger, 2005).

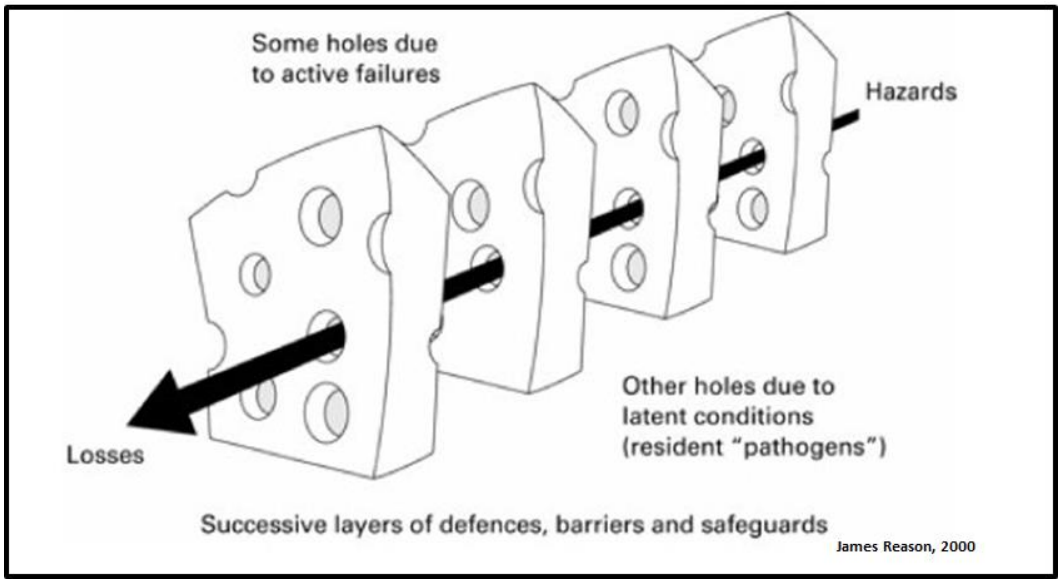


Figure 2: Reason's Theoretical Model of Accident Causation (Resiliency Model)

In his "Human Error: Models and Management" article, Reason reported that, in a complex system such as healthcare, human error is likely to occur and that expecting perfection from imperfect human beings, or punishing them for their mistakes will not improve safety. The model indicates that the preferred strategy is either to prevent an error from occurring or prevent the error from causing harm through the application of multiple steps that function as a safeguard net (Reason, 2000).

Reason's model serves as a strong foundation for developing a comprehensive management framework that strengthens security safeguards and mitigates threats to protect patient record from breaches. Information security systems adopt multi-layered defense approaches, incorporating measures such as identity access and user authentication management, intrusion detection systems, antivirus software, user awareness programs, employee training, and compliance with government regulations. In the application of the model to healthcare information security, each defense layer aligns with Reason's Resiliency Model, where multiple safeguards work together to prevent breaches. Applying this model as a platform for studying human error in EHR information security enables an assessment of the effectiveness of individual security layers, as well as the combined impact of multiple layers in preventing successful data breaches.

Alternatively, the Domino Theory and other event chain models, such as Failure Modes and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Event Tree Analysis, and Cause-Consequence Analysis, are limited in their capability to explain accident causation from persistent, increasingly sophisticated, and evolving threats such as malicious cyber campaigns against healthcare systems (Leveson, 2004). The Domino Theory, proposed by Heinrich in the 1940s, describes an accident as a chain of discrete events which occur in a particular temporal order. It is designed to help practitioner identify intervention points, points that, if acted on, will yield a more favorable outcome, such as no accident or an event that does not lead to injury or property damage (Heinrich, 1980) (Qureshi, 2008).

The Information Security Theory, which aims to protect systems from vulnerabilities or accidents, often overlooks the role of human behavior creating system vulnerabilities. The theory tends to rely on a structured approach to risk management, which presents challenges given the evolving nature of cyber threats that require continuous adaptation and flexibility. The theory focuses on safeguarding business continuity by reducing or eliminating the effect of security incidents (Von Solms, 1998). According to the theory, the primary objective of any information security system is to preserve the confidentiality, integrity, and availability of business or personal information (McCumber, 1991), (Posthumus et al., 2004).

1.3 Enhancement of Reason's Resiliency Model: Integration of Reason's Model and STS Management Framework

"If you think technology by itself can solve your security problems, then you don't understand the problems, and you don't understand the technology," Bruce Schneir.

Socio-Technical Systems (STS) principles emphasize that human agents and social institutions are not just additions to technical systems but integral components for their success (Charitoudi, 2013). STS is an approach to complex organizational work design that considers requirements from the interaction between people, technology, government policy, and organization aspects in workplaces.

Organizational objectives are not met by the optimization of the technical system alone, but by the joint optimization of the technical, human, and social factors. Highly technological systems such as telecommunications, defense, and healthcare and patient safety are exceedingly becoming more complex (Qureshi, 2008). In these systems, humans interact with technology and deliver outcomes as a result of their collaboration; such outcomes cannot be attained by either the humans or technology functioning in isolation. These systems comprised of human agents and technical artefacts, are often embedded within complex social structures such as the organizational goals, policies and culture, economic, legal, political and environmental realities.

The application of STS principles associated with human error in information technology and the cybersecurity domain has not received much attention (Charitoudi et al., 2013). Most emphasis to solve healthcare information security incidents has been placed by considering technical solutions with marginal attention to solving the challenges presented by the human-technology interactions in the organization (Malatji et al., 2019). Healthcare organizations are extraordinarily complex, with many typical extreme organizational characteristics that include a technology saturated environment, internal politics, regulatory pressures, and a patient-centered care (Smet, 1982). Given the complexity of healthcare organizations, several studies acknowledge that simple models based on robust technical design solutions are insufficient to prevent healthcare data breaches.

This dissertation presents a more socially oriented management framework (Figure 3) that applies STS principles to the human-technology interface error challenge in healthcare. This framework represents a cultural shift from the sector's current reliance on purely technical design solutions toward a socio-technical design environment. The process of leading cultural change violates the assumptions that normally guide our interactions with others. Thus, simply telling organizations about that process will not show them why it works since the explanation just bounces off of their strongly held normal assumptions (Quinn, 2012). Based on this consideration, to effectively influence

a change in culture, the sector's cyber professionals should be put through their security incident experiences to cause them to challenge their own assumptions. They should carefully examine what is currently occurring during major human error data breach incidents and apply lessons learned to create long term resilience capabilities.

The proposed framework builds on Reason's Resiliency Model, adopting his layered design approach while integrating STS factors identified in the literature as effective in reducing human error-related data breaches. The layer approach utilizes historical data on STS factors such as investments in identity and access management (IAM) capabilities, employee training initiatives, and the adoption of zero-trust principles, to empirically assess their effectiveness as safeguard layers. The framework assesses the effectiveness of these safeguard layers in mitigating human error-induced data breaches and enhancing the resilience of healthcare IT systems.

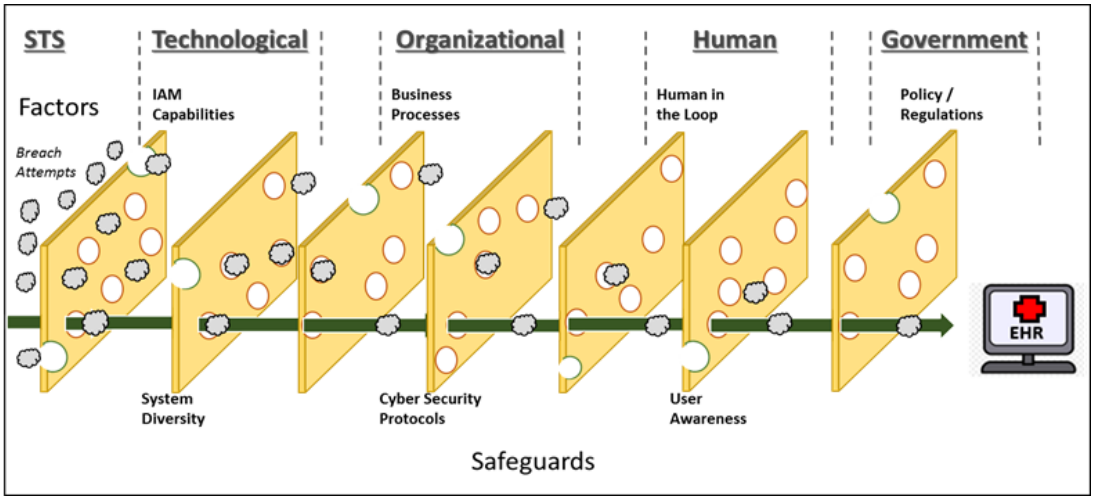


Figure 3: Integration of STS Management Framework and Reason's Resiliency Model

1.4 Dissertation Framework

The purpose of this research dissertation is to study the impact of error, as a consequence of the human-technology interface, in the information security of the healthcare sector. In this context, ***I have selected the impact of human error data breaches on EHR information security as the research focus for this dissertation.*** The significance of the problem is undisputable, as the present day healthcare industry

has become the main victim of external and internal cybersecurity incidents with some major publications reporting that over 80% of all data breaches are caused by an employee mistake, despite continuous investments in cybersecurity for addressing the problem.

The literature demonstrates the value of adoption of EHR technology to improve healthcare quality of services, as well as strong evidence that information security ranks at the top of all challenges faced by the healthcare industry. Since, the implementation of EHR's technology demands protecting the privacy and security of patients' healthcare information, and the trends of data breaches resulting from human error suggest improvements in healthcare information systems, this problem setting presents a unique opportunity to address the research purpose of this dissertation.

This dissertation integrates three strands of literature to develop a comprehensive understanding of the overall research topic. Figure 4 illustrates the outcome of these essays combined to enhance Reason's Resiliency Model. The three key strands include: human error in healthcare information security; human error data breaches as an unintended consequence of EHR technology adoption; and government regulation as a safeguard to prevent human error in information security.

This dissertation is structured into these three essays, each examining the impact of human error data breaches on EHR information security, offering insights into the role of human, technological, and government regulatory factors for mitigating these risks. The first essay presents a literature review on human error as a key contributing factor to EHR data breaches. The second essay examines the unintended consequences of EHR technology adoption, focusing on its impact on productivity within state healthcare systems. The third essay integrates government regulation into Reason's Resiliency Model, incorporating HIPAA policy as a safeguard layer to prevent data breaches from escalating into full-scale security incidents.

While each essay addresses a distinct issue, they share a common Socio-Technical Systems (STS) management framework to analyze the interactions between technological, organizational, human, and government regulatory factors. This integrated approach enhances Reason's Resiliency Model by incorporating STS factors, ensuring a comprehensive resilience framework that strengthens safeguards against potential threats to EHR information security.

Essay 1 focuses on understanding the root cause and impact of human error in healthcare organizations, drawing knowledge from the Human Factors Engineering and Reason's theories on safety and resilience engineering. Essay 2 focuses on the unintended consequences of EHR technology adoption and their impact on healthcare performance. This essay is informed by economic production theory. Essay 3 explores the effectiveness of Government HIPAA policy as a safeguard layer to prevent data breaches. This essay is informed by Systems Thinking and Reason's theory on safety and resilience engineering. Additional insights on how these three strands of literature come together to support the dissertation research is included in the following sections.

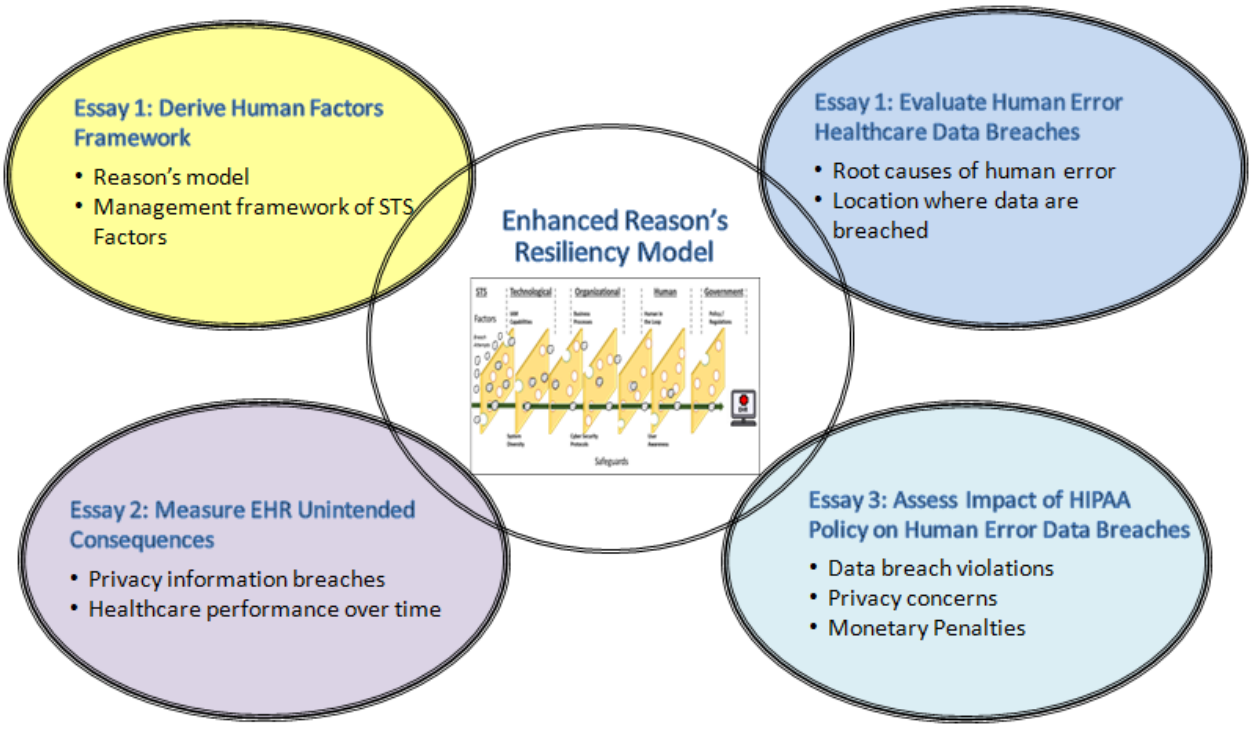


Figure 4: Combination of Essay Outcomes to Enhance Reason's Resiliency Model

Figure 5 presents the dissertation framework with the structure, research questions, hypotheses, and methods for the three essays investigated in this research and described in the sections below.

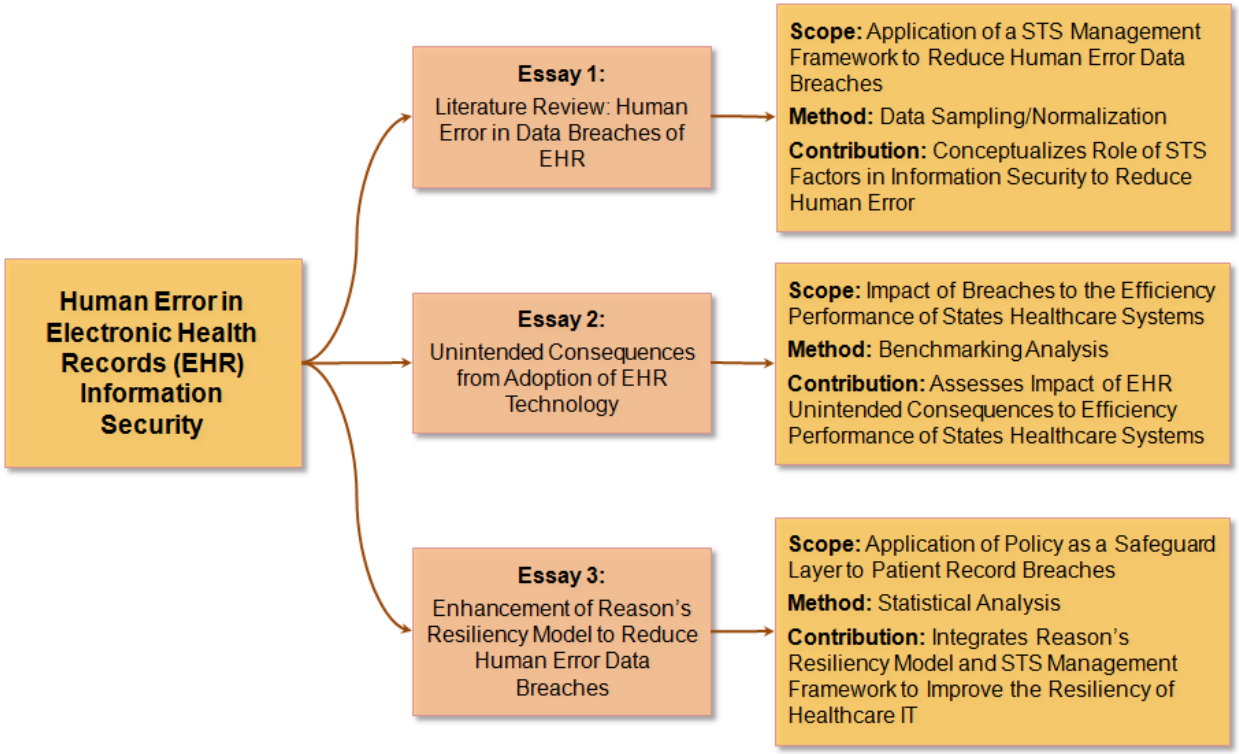


Figure 5: Dissertation Framework - Structure, Scope, Method, and Contribution

1.4.1 Essay 1 examines literature findings on Human Factors Engineering theory, Reason's Theory of Accident Causation, and real-world data on human-technology interface errors responsible for EHR data breaches. The analysis is based on a systematic literature review and an evaluation of data collected from the DHHS OCR, which documents healthcare data breach incidents where 500 or more records were compromised.

This essay develops a taxonomy of the predominant human errors contributing to the rise in data breaches, and introduces a management framework that applies STS principles to address the human-technology interface challenge in the healthcare sector. The hypothesis tested in this essay states that, **the location where data are breached within healthcare IT systems, as a consequence of errors from the human-technology interface, significantly influence the severity of data breaches**

impacting the security and privacy of patient records. Empirical data from DHHS OCR is used to assess the locations where data breaches occur and their relative impact on the number of compromised patient records.

1.4.2 Essay 2 studies the literature on Economic Production Theory to evaluate the unintended consequences of EHR technology adoption. Specifically, it measures the impact of information privacy concerns stemming from human error-related data breaches on the productivity performance of patient care services. While the adoption of EHR technology aims to improve the productivity of healthcare systems, human error-related data breaches results in: disruptions to patient care services due to healthcare organizations limiting or suspending access to compromised systems which can delay critical medical procedures and lead to longer wait times for patients; financial liabilities and resource reallocations to payments of fines and legal costs; and, patient compensation which in many instances were initially intended for system improvements and productivity enhancements and or data breach mitigations.

Building on the findings from Essay 1 regarding information privacy concerns linked to EHR-related human errors, this essay investigates their effects on the productivity performance of healthcare providers. The Malmquist Productivity Index (MPI) is used to measure productivity changes over time across decision making units (DMUs). A table outlining the proposed input and output variables is presented in Table 21 of this dissertation.

This essay tests the hypothesis that, **despite increasing patient privacy concerns due to healthcare data breaches, the adoption of EHR technology has contributed to productivity improvements in DMUs through technological advancements and efficiency gains.** DMUs are represented by state healthcare systems categorized into three main groups: high-capacity states, mid-capacity states, and low-capacity states. To assess this hypothesis, a hybrid approach integrating benchmarking and statistical analyses was utilized.

1.4.3 Essay 3 examines the impact of HIPAA policy compliance as a security safeguard against human error-related data breaches in EHR systems. It integrates the STS Management Framework developed in Essay 1 (Figure 12) with Reason's Resiliency Model (Figure 2) to assess the effectiveness of HIPAA policy as a security safeguard layer in reducing the number of compromised patient records.

Since HIPAA non-compliances result in monetary penalties, this essay tests the hypothesis that, **HIPAA monetary penalties are positively correlated with a reduction in the number of compromised patient records.** To evaluate this relationship, statistical regression models with lagged explanatory variables are employed. The results of this analysis are presented in Chapter 4 of this dissertation.

1.5 Research Contributions and Overarching Impact

"The mere formulation of a problem is often far more essential that its solution, which may be merely a matter of mathematical or experimental skill."

- Albert Einstein (Physics Nobel Price, 1921).

This dissertation contributes to the literature of human-technology interface, its impact on errors, and on healthcare information security. Even though these topics have caught the attention of many researchers and healthcare stakeholders, this dissertation takes a unique and unexplored stance by applying Reason's Resiliency Model and analyzing the latest real-world data collected on healthcare security incidents to test the theory and expand its application to human error management in the information security domain. The dissertation enhances understanding of the unintended consequences of technology adoption, particularly regarding patient information privacy and data breaches. Furthermore, it assesses the effectiveness of HIPAA policy designed to protect patient health information.

An important contribution from this research are the unique qualitative and quantitative datasets used for modeling and testing hypotheses testing the three essays in the dissertation.

The qualitative data is derived from semi-structured interviews with subject matter experts (SMEs) across multiple fields, providing insights that inform model formulations, validation processes, and the interpretation of findings and recommendations. Appendices F thru J include the protocols, questions and data structure, and the results associated with the semi-structured interviews used to collect the qualitative data to support the dissertation.

Comprehensive quantitative datasets of real-world healthcare IT data support the modeling and hypothesis testing conducted to address the research questions in each essay. These datasets include the most recent data on cybersecurity incidents affecting healthcare information technology systems across multiple entities, including hospitals, private practices, and health insurance providers. Additionally, they incorporate healthcare performance metrics, demographic information, and economic data. These data come from multiple government entities, including DHHS, U.S. Census Bureau, the National Center for Health Statistics, the American Hospital Association, and, state health departments. Appendix A includes a list of all quantitative datasets used in this dissertation.

Essay 1 contributes to the Human Factors Engineering Theory and Reason's Theory of Accident Causation by developing two management frameworks for addressing the impacts of human error data breaches in the healthcare information security domain. The literature identifies the need for further research to investigate the impacts of STS factors on the reduction of human errors in information security. To address this gap, Essay 1 developed a management framework of STS factors that drive human error (Figure 12) to conceptualize the roles of STS factors in the information security-theater and improvements needed to reduce errors.

To advance the understanding of the human factors engineering and Reason's theory, Essay 1 develops a taxonomy of human error root causes in information security. This taxonomy investigates the predominant human errors that are contributing to the proliferation of data breaches and the barriers that are slowing down EHR adoption and

information sharing in the healthcare sector. The taxonomy drills down to the root causes of human-technology interface errors to evaluate the unintentional, intentional, and malicious employee behaviors that lead to human error data breaches, compromising the security of patient healthcare records.

Essay 1 also applies these frameworks to assess the impact of human error on data breaches, focusing on the significance of the location where data are breached and the severity of these breaches to patient privacy. This analysis has real-world implications for healthcare data security. Identifying where data is most vulnerable to human error-related breaches enables organizations to: (1) develop more effective incident response and containment strategies to minimize breach impact, shorten the data exposure timeframe, accelerate the restoration of patient care services, and reduce overall breach costs; and, (2) optimize resource allocation by prioritizing efforts to mitigate recurring human errors and their associated data breach risks. This contribution has the potential to enhance information security, lower associated costs, and reduce the number of compromised patient records.

Essay 2 contributes to the Economic Production Theory and technology management literature by highlighting the impact of unintended consequences, such as breaches to patient private information, stemming from EHR technology adoption in healthcare organizations. These unintended consequences lead to disruptions in patient care services and financial liabilities, forcing organizations to reallocate resources to mitigate their impact to restore normal operations. This essay examines how these consequences influence organizational productivity over time, particularly within complex system environments like healthcare. In the MPI calculations, these unintended consequences are represented as input variables, specifically data breach incidents reported by the DMUs.

This essay makes important contributions to the Economic Production Theory, particularly in the context of digital transformation efforts aimed at enhancing patient care efficiency. Despite ongoing investments in information technology, patient healthcare information continues to be vulnerable, highlighting a critical area for further

exploration and improvement. The empirical analysis, utilizing the latest data on cybersecurity incidents affecting healthcare IT systems, offers valuable insights to understand healthcare IT system vulnerabilities. These findings may generate further research questions on this critical topic and its wider economic implications for the healthcare sector.

Essay 3 contributes to the Resiliency and Safety Engineering theories. It enhances Reason's Resiliency Model by integrating a STS management framework into its layered approach to mitigate human error challenges in healthcare information security. The essay also test the effectiveness of the HIPAA policy, as a security safeguard or layer, aimed at reducing the incidence of successful data breaches and the compromise of patient healthcare records.

The findings from this essay highlight the importance for organizations to prioritize the development and enforcement of safeguards that align with HIPAA policy to protect healthcare data integrity. This is important for maintaining patient trust and minimizing the burden of future financial penalties and legal consequences. Additionally, the essay offers a series of recommendations, beyond monetary penalties, that the government can implement to strengthen HIPAA compliance and mitigate the risk of data breaches resulting from human error.

1.6 References

[1] Blumenthal, D., Guman, E., Williams, R., (2024). Why the U.S. Healthcare System is So Much Worse than Its Peers. Harvard Business Review.

[2] Bowman, S., (2013). Impact of Electronic Health Record Systems on Information Integrity: Quality and Safety Implications. AHIMA.

[3] Bush, G., (2006). 2006 State of the Union Speech. The White House.

[4] Charitoudi, K., Blyth, A., (2013). A Socio-Technical Approach to Cyber Risk Management and Impact Assessment. Scientific Research.

[5] Davis, J., (2021). Healthcare Accounts for 79% of All Reported Breaches, Attacks Rise 45%. Health IT Security.

[6] Gesulga, J.M., Berjame, A., Moquiala, K.S., Galido, A., (2018). Barriers to Electronic Health Records System Implementation and Information Resources: A Structured Review. Scopus Elsevier.

[7] Heinrich, H. W., Petersen, D., Roos, N., (1980). Industrial Accident Prevention. New York: McGraw-Hill.

[8] Health Insurance Portability and Accountability Act (HIPAA), (2021). Healthcare Data Breach Statistics. Department of Health and Human Services [19]Leveson, N.G., (2004). A New Accident Model for Engineering Safer Systems. Reading. MA: Addison Wesley.

[9] Leveson, N.G., Daouk, M., Dulac, N., Marais, K., (2003). Applying STAMP in Accident Analysis. Semantic Scholar.

[10] Malatji, M., Sune, V.S., Marnewick, A., (2019). Socio-Technical Systems Cybersecurity Framework. Emerald Publishing Limited.

[11] McCumber, J., (1991). Information Systems Security: A Comprehensive Model. Proceedings of the 14th National Computer Security Conference, Washington: National Institute of Standards and Technology. National Computer Security Center.

[12] Perneger, T.V. (2005). The Swiss Cheese Model of Safety Incidents: Are There Holes in the Metaphor? BMC Health Services Research.

[13] Ponemon Institute, (2024). Cost of a Data Breach. International Business Machines (IBM) Report on Security.

[14] Posthumus, S., Von Solms, R., (2004). A Framework for the Governance of Information Security. Computers & Security (23:8), pp 638-646.

[15] Quinn, R., (2012). Deep Change Field Guide. Jossey Bass, John Wiley & Sons Inc.

[16] Qureshi, Z.H., (2008). A Review of Accident Modelling Approaches for Complex Critical Socio-Technical Systems. Defense Science and Technology Organization.

[17] Reason, J., (2000). Human Error Models and Management. British Medical Journal (BMJ).

[18] Smet, M., (1982). Cost Characteristics of Hospitals. Social Science & Medicine. Europe PubMed Central (PMC).

[19] Statista, (2024). Cybersecurity – United States. Statista.

[20] Von Solms, R., (1998). Information Security Management (3): The Code of Practice for Information Security Management (Bs 7799). Information Management & Computer Security (6:5), pp 224-225.

[21] Yan, Z., Robertson, T., Yan, R., Park, S.Y., Bordoff, S., Chen, Q., Sprissler, E., (2018). Finding the Weakest Links in the Weakest Link: How Well Do Undergraduate Students Make Cybersecurity Judgment? Scopus Elsevier.

[22] Zimmermann, V., Renaud, K., (2019). Moving from a “Human-as-Problem” to a “Human-as-Solution” Cybersecurity Mindset. Scopus Elsevier.

Appendix A
Dissertation Quantitative Datasets with Sources and Data Range

Data by State	Category	Range	Source
Population	Demographics	1997-2022	Department of Commerce (DoC)- Census Bureau's American Community Survey (ACS)
Gross Domestic Product (GDP)	Economics	1997-2022	DoC- U.S. Bureau of Economic Analysis (BEA)
GDP per Capita	Economics and Demographics	1997-2022	DoC- U.S. Bureau of Economic Analysis (BEA)
Healthcare Expenditure	Healthcare Economics	1991-2022	DHHS- Centers for Medicare & Medicaid Services, Office of the Actuary, National Health Statistics Group
Healthcare Expenditure per Capita	Healthcare Economics and Demographics	1991-2022	DHHS- Centers for Medicare & Medicaid Services, Office of the Actuary, National Health Statistics Group
Healthcare Expenditure as a % of GDP	Healthcare Economics and Demographics	1991-2022	DHHS- Centers for Medicare & Medicaid Services, Office of the Actuary, National Health Statistics Group
Cost by Healthcare Services (ex. Dental, Home Health, Nursing)	Healthcare Economics	1991-2020	DHHS- Centers for Medicare & Medicaid Services, Office of the Actuary, National Health Statistics Group
Patients' Health Insurance (Employer, Military, Medicaid, Uninsured)	Healthcare Services and Demographics	1999-2022	DoC- Census Bureau's American Community Survey (ACS)
State Healthcare System Characteristics	Healthcare Services	Current	States Health Departments
Physicians and Clinical Services	Healthcare Services	1991-2020	DHHS- Centers for Medicare & Medicaid Services, Office of the Actuary, National Health Statistics Group
Hospitals by Type	Healthcare Services	1991-2020	American Hospital Association (AHA) Annual Survey
Hospital Admissions	Healthcare Services	1999-2022	American Hospital Association (AHA) Annual Survey
Hospital Admission per Capita	Healthcare Services and Demographics	1999-2022	American Hospital Association (AHA) Annual Survey
Hospital Outpatient Visits	Healthcare Services	1999-2022	American Hospital Association (AHA) Annual Survey
30 Day Hospital Readmissions	Healthcare Services	2020-2022	American Hospital Association (AHA) Annual Survey
Length of Stay	Healthcare Services	1999-2022	American Hospital Association (AHA) Annual Survey
Emergency Room Visits	Healthcare Services	1999-2022	American Hospital Association (AHA) Annual Survey
Hospital Inpatient Days	Healthcare Services	1999-2022	American Hospital Association (AHA) Annual Survey
Hospital Outpatient Visits	Healthcare Services	1999-2022	American Hospital Association (AHA) Annual Survey
Health Professionals (Physicians, Nurse Practitioners)	Healthcare Services	2024	Redi-Data Inc.
Managed Patients	Healthcare Services	1999-2022	American Hospital Association (AHA) Annual Survey
Life Expectancy	Health Status	1959-2020	National Center for Health Statistics
Deaths	Health Status	2000-2022	DHHS -Centers for Disease Control and Prevention's National Center for Health Statistics
Mortality Rate	Health Status	2000-2022	DHHS -Centers for Disease Control and Prevention's National Center for Health Statistics
Hospital Adoption of EHRs	Business Process Modernization	2009-2020	DHHS -Centers for Disease Control and Prevention's National Center for Health Statistics
Healthcare Nursing Facilities Adoption of EHRs	Business Process Modernization	2009-2019	DHHS -Centers for Disease Control and Prevention's National Center for Health Statistics
Data Breach Incidents	Information Security	2009-2024	DHHS- Office of Civil Rights
Patient Records Compromised	Information Security	2009-2024	DHHS- Office of Civil Rights
HIPAA Violations -Monetary Penalty Settlement	Information Security and Policy	2009-2024	DHHS- Office of Civil Rights

Chapter 2.0 - Essay 1: Systematic Literature Review- Human Error in Data Breaches of Electronic Health Records (EHR)

Abstract

This chapter introduces a conceptual framework of the STS factors that are hypothesized to reduce human error data breaches in the healthcare sector. The framework addresses a research gap from the literature in terms of understanding and modeling of human-computer interactions and the consideration of STS factors when developing solutions.

A systematic literature review was conducted, analyzing 1,071 documents to inform the research. From this review, two conceptual frameworks were developed: a taxonomy categorizing human errors leading to data breaches and a management framework based on STS principles. The findings identified a gap in terms of understanding and modeling of human-computer interactions, as well as the need for greater consideration of STS factors when designing information security solutions.

Human errors are a growing threat to EHR technology adoption and information sharing. Healthcare data breaches and criminal attacks continue to increase in volume and complexity. To fully realize the benefits of EHR technology, the industry must acknowledge the critical role of human-technology interface errors in cybersecurity and prioritize the protection of health information. Semi-structured interviews with SMEs were used to collect qualitative data to support this research study. The interviews were designed to provide a better understanding of the role of human error in data breaches and to inform the hypothesis testing.

The STS management factors are used to determine how the location where data are breached influence the number of compromised patient records. The findings reveal that network servers and emails are the two most common sites where healthcare data are breached capturing 95% of all compromised patient records since 2009.

KEYWORDS: Computer Security, Cybersecurity, Data Breaches, Data Envelopment Analysis, Electronic Health Records, Healthcare, Human Error, Methods, Risk, Socio-Technical Systems (STS).

2.1 Introduction

This essay presents the findings of a literature review of the STS factors that influence human errors in EHR data breaches. EHR store all or parts of patient's health information in a digital form. They are digital records that are intended to provide a comprehensive view of a patient's medical history. A healthcare data breach occurs when a patient's name, combined with his/her medical record, is exposed, whether electronically or on paper, potentially putting information at risk (Megas et al., 2015), (Rouached et al., 2011); (Hofmey, 1999). Human error, an unintended action resulting in unacceptable consequences, can lead to security breaches and deter EHR adoption and information sharing. However, findings from the literature review suggest that mitigating human error should be part of system design and data security review efforts (Palabindala et al., 2016).

The healthcare sector must improve its efforts to protect patient information from cyber-attacks. Healthcare cyber professionals must carefully examine what is occurring during major data breach incidents and apply lessons learned to strengthen infrastructure resilience (Alvarado, Triantis, 2024). However, this proposition is not as easy to implement as it sounds. Healthcare organizations are extraordinarily complex, characterized by a technology-saturated environment, internal politics, regulatory pressures, and a patient-centered care model (Smet, 1982). Given this complexity, protecting the information systems require more than robust technical design solutions, government policies, and regulatory actions. It requires a shift in how the sector approaches healthcare data security (Alvarado, Triantis, 2024).

Relying solely on technical alternatives might not be sufficient to enhance the security of healthcare records. Instead, applying socio-technical systems (STS) principles to information security introduces a comprehensive approach that integrates government policy, human in the loop, organizational processes, economic factors, and technical factors, along with the interrelationship among them. STS is an approach for designing complex organizational systems that considers the dynamic interactions between people, technology, government regulations, and organizational structure aspects in the

workplace. By leveraging this approach, the impact of human error in data breaches can be reduced (Alvarado, Triantis, 2024).

This essay introduces a conceptual framework of STS factors that cause human errors in data breaches. It is argued that the study of complex systems such as EHR should consider the interactions and relationships between technology, organization processes, people, and government policy. The framework is based on information found from a systematic literature review of over 1,000 articles conducted for this dissertation. It highlights key STS factors that influence human-technology interface error and their impact to data security: Identity Access Management (IAM) Capabilities; System Diversity; Business Processes; Cyber Security Protocols; Human in the Loop; User Awareness; and, Government Regulations (Alvarado, Triantis, 2024).

Many STS factors that contribute to human error causing data breaches in healtcare systems are closely related. The analysis performed in the literature review began by listing all of the factors and attributes identified by the publication authors that probably contribute, at varying degrees, to increasing the likelihood of data breaches not only in hospitals but in healthcare organizations such as private practices, health insurance organizations, and treatment and medical test facilities. The STS factors selected for the management framework specifically excludes technical risk-drivers such as encryption protocols, software cyber detection applications, and firewalls, which are typically captured by the inherit design of hardware infrastructures and most commercial EHR software applications found in industry. The selection of these STS factors described in the sections below was informed by the analysis of over 1,000 papers as part of a systematic literature review (Alvarado, Triantis, 2024).

IAM- Strong IAM solutions are a necessary component of an information security system. Organizations that keep a close audit and monitoring of their devices authorized for conducting official business, are better positioned to avoid malware and can respond to incidents faster than organizations that don't follow this practice (Megas et al., 2015).

System Diversity- The EHR vulnerability of the U.S. healthcare sector is affected by the vulnerabilities of all individual healthcare units. In this large system, reducing variability of individual healthcare units will make the whole system less vulnerable. Networked or connected medical devices have become a popular practice in healthcare to remotely monitor patients, deliver care, and transfer patient data. A common capability framework focused on reducing human technology interface errors will make the healthcare industry less attractive to cybercriminals (Jalali et al., 2018).

Business Processes- Cybersecurity threats and data breaches in the healthcare sector are far from over. The healthcare sector needs to be prepared and proactive to respond to data breaches, protect their reputation, and lessen the financial burden associated with identifying and responding to a data breach (Basset et al., 2021). Given the sensitivity of patient' information, healthcare management efforts should strive to create an organizational security culture environment, where employees feel the responsibility of immediately reporting mistakes or unintentional disclosures of patient's data without fear of repercussion (Hung, 2010). Even when the mistakes or disclosures might not be reversed, their impact might be mitigated and the end damage to the organization and patient's data be diminished (HIPAA, 2021).

Cyber Security Protocols- People make mistakes. Most errors are unintentional actions, typically taken by an internal or insider threat actor, but partner actor errors also occur. The trend of basic human error in the healthcare industry is not diminishing. Lack of following cybersecurity protocols such as neglecting two-factor authentication is making it easier for cyber criminals to get unauthorized access to secure systems (University of Illinois, 2020). Healthcare data breaches today are primarily the result of employee unintentional errors that leads to unauthorized access to records that could be preventable if the appropriate cybersecurity protocols are deployed. It is therefore critical for healthcare management to focus on elevating cybersecurity protocols in their information security risk management plans (Ponemon Institute, 2022).

Human in the Loop- Healthcare information technologist have raised concerns that although human behavior and their errors often lead to data breaches and present a barrier for EHR adoption and information sharing (Gesulgaa et al., 2018), despite repeated calls for human factors to be addressed in the design of IT systems the issue has not adequately been addressed by many current security models (Tellez Isaac et al., 2011). In the information security theory, humans are seen as the weakest link in the security chain (Yan et al., 2018). The variability on the probability of human error has a significant importance in reducing the healthcare unit vulnerability to data breaches. People are a vital part of protecting the privacy of patients' EHR. An organizational culture shift, focused on human-computer interaction, which integrates medical professional staff in the design of security capabilities rather than treating them as their weakest point, could result in the reduction of cyber incidents leading to data breaches (Zimmerman et al., 2019).

User Awareness- The greatest threat to EHR lies with the unintentional and sometimes malicious actions of unmotivated users with open access to information resources (Warketin et al., 2009 & 2013). Awareness about the damaging consequences of cybersecurity incidents is key for employees to be cognizant about security while executing their daily tasks (Dinella et al., 2021). For example, many HIPAA breaches result from employee's lack of awareness on their data security obligations or making basic mistakes under time pressure or stress due to excessive workloads. Employee awareness training that focus on common cybersecurity incidents problem areas and the latest data security policies and procedures, will create an environment where healthcare staff be more conscious about their roles and will reduce the likelihood of occurrence of human error in EHR data breaches (Palabindala et al., 2016).

Regulations- Continuous enforcement of Government policy such as HIPAA has been a driving force behind healthcare organizations' creation of protocols for prevention, detection, and remediation of reported incidents (HIPAA, 2021). Government regulation have made an impact on the operation of healthcare providers and providing safeguards to protect the information integrity contained in EHR. Government oversight,

in the form of policy regulation, is necessary to ensure healthcare enforcement and compliance of protected health information security standards to avoid information security issues resulting from unintentional consequences from EHR use (Bowman, 2013).

2.2 Technical Background

"The problem of human error can be viewed in two ways: the person approach and the system approach. Each has its model of error causation, and each model gives rise to different philosophies of error management." James Reason (Human Error: Models and Management, 2000).

This chapter explores the Human Factors Engineering Theory and the Reason's Accident Causation Theory. The study of these theories focus on human performance and interaction with equipment, systems and processes within the organization. Their goal is to enhance performance, improve safety, and increase user satisfaction (Milligan, 2007). In his Resiliency Model Theory, Reason presents human error as a two prong approach: the person approach and the systems approach. Each approach represents a different model of error causation, leading to different philosophies of error management (Reason, 1990).

The literature provides statistical evidence linking data breaches caused by human-technology interface errors to challenges in EHR adoption and secure information sharing (HIPAA, 2022). Research suggests that addressing this security threat requires a fundamental shift in the healthcare sector's approach to data security. Such a shift necessitates a deep understanding of the theories and principles underlying human error. To support this change, Essay 1 begins by reviewing a taxonomy of human errors and developing a management framework based on STS factors identified in the literature. This framework serves as a foundation for analyzing the root causes of human error and understanding the motivations behind breaches in information security.

The application of STS principles to human error in information technology and the cybersecurity domain has not received much attention (Charitoudi et al., 2013). While numerous journal articles explore cybersecurity challenges in the healthcare sector;

only very few studies, (Warkentin et al., 2017), (Ponemon Institute, 2020) and (Pfleeger et al., 2012), address the implications of human errors on data breaches of patient healthcare records. Despite significant investments in information security hardware and software solutions, human error continues to increase, contributing to frequent data breaches and compromising millions of patient PHIs at an alarming rate.

To complement the historical healthcare quantitative data used to test this hypothesis, this review incorporates insights from the systematic literature review to get a better understanding of the real knowledge of STS factors and their implication to information security. Table 1 presents selected publications from the systematic literature classified by subject areas.

Subject Area	***Literature on Information Security Human Errors***
Communications	10
Human and Social Factors	23
Information Systems	22
Management Science	6
Modeling	6
Operations	12
Safety and Risk Analysis	12
Science	1
Technology & Engineering	13
Theory and Policy	1
Total	***106***

Table 1: Publication Trend of Human Error in Information Security by Subject Area

2.3 Research Problem

The U.S. healthcare sector continues to face persistent and increasingly sophisticated malicious data breach attempts, posing significant risks to the adoption and widespread information sharing of EHR systems across both the public and private sectors. The rise in cybersecurity incidents, particularly EHR data breaches, presents challenges for the healthcare industry as a whole, with hospitals being especially vulnerable (Callahan, 2013). These threats ultimately endanger patients' PHI. According to the 2024 HIPAA Journal, data breaches in the healthcare sector have steadily increased over the past decade. In 2023 alone, a record-breaking 733 breaches were reported, each involving

the compromise of more than 500 patient records. The journal also highlighted notable shifts in the identified root causes of these breaches (HIPAA, 2024).

EHR adoption and information sharing present a unique opportunity to enhance the productivity of the healthcare. However, this enhancement can only be realized if robust information security systems are implemented to protect patient data from both insider threats and external malicious actors. Protecting patient safety and sensitive information requires a change, one that acknowledges cybersecurity as an integral component of patient care.

Healthcare data breaches are increasingly difficult to identify and are occurring at alarming rates (Dolezel et al., 2019). Over the past two decades, researchers have made various scientific attempts to identify, classify, and mitigate vulnerabilities within healthcare organizations (Razaque et al., 2019). However, a report from IBM Security (Ponemon Institute, 2022) indicates that it still takes an average of nine to twelve months to identify and resolve a data breach incident. The same study showed that the quicker a breach is identified and resolved, the lower the cost impact on healthcare organizations.

Per the literature (Gabriel et al, 2018), the most common identified locations of healthcare data breaches include eight categories: emails; desktop computer; electronic health records; paper/films records; laptop computers; network server; other portable devices, and other locations. Data breaches in these locations are attributed to vulnerabilities found in multiple STS factors within the healthcare IT systems.

For example, the lack of reliable identity access management (IAM) solutions, coupled with diversity between IAM capabilities across healthcare units, contribute to vulnerabilities in the EHR system, increasing the risk of unauthorized access to network servers. Similarly, breaches involving unsecured health information from emails and paper/films records often result from the absence of strong business processes and insufficient user awareness training, leading to unintentional disclosures to unauthorized

parties. Additionally, resource constraints prevent healthcare organizations from allocating sufficient budgets to establish cybersecurity protocols that monitor desk top computers and external devices, integrate human in the loop approaches in security safeguard designs, and ensure compliance with government regulations to prevent unauthorized disclosures. These factors collectively highlight the systemic challenges in protecting healthcare data from breaches.

While these vulnerabilities have always existed, the alarming rate at which they are being exploited is a growing concern. To respond to these threats, this chapter examines the relative significance of specific breach locations within healthcare IT systems. The essay will test the hypothesis that, **the locations where data are breached within healthcare IT systems, as a consequence of errors from the human-technology interface, significantly influence the severity of data breaches impacting the security and privacy of patient records.** The findings of this essay have the potential to help management develop more effective incident response and containment strategies, reducing the lifecycle of data breaches, enabling faster restoration of patient care services, and lowering associated costs. Additionally, the insights gained could support more strategic resource allocation, prioritizing the development of safeguard layers and influencing government policies aimed at mitigating recurring human errors and minimizing the impact of data breaches.

As a result of the modeling and analysis of the data, this essay is set to address the following question, ***to what extent do the locations where data are breached within healthcare IT systems, as a consequence of errors from the human-technology interface, contribute to the severity of these breaches impacting the privacy of patient records?***

2.4 Research Method

2.4.1 Data

Qualitative data and quantitative datasets are used in this essay to support modeling and data analysis of the foundational data for Chapters 2 of this research.

Qualitative Data Collection- Semi-Structured Interviews

Semi-structured interviews with subject matter experts (SMEs) enabled the collection of qualitative data to support this research study. Information obtained from the semi-structured interviews provided real world qualitative data to validate results found in the literature and support the hypotheses testing of the three essays of this dissertation. The interviews were designed to provide a better understanding of the role of human error in data breaches; gain insights into the unintended consequences of IT adoption such as human error data breaches on the productivity performance of patient care services; and, obtain a perspective from stakeholders on the effectiveness of HIPAA policy reducing breaches in the sector. Appendices F thru J include the semi-structured interview protocols with interview questions and structure followed, list of SMEs and their associated expertise by STS factor, responses to questions, summary of results, and the Virginia Tech Institution Review Board (IRB) request and approval forms.

Figure 6 and Table 2 illustrate the selection of subject SMEs from various organizations within the healthcare sector, cybersecurity field, and policy professions for the semi-structured interview sessions. These SMEs were chosen based on their expertise in one or more factors within the STS management framework, which is utilized to enhance Reason's Resiliency Model, as presented in Figure 12.

Figure 6: SMEs Provided Real World Qualitative Data to Support this Research Study

Interview with eight SMEs were conducted in the following domain areas:

STS Factor	Expertise Field	SME
Identify Access Management (IAM)	**Cybersecurity**	A program manager developing an IAM program for protecting national security data
System Diversity	**Cybersecurity**	A cybersecurity system designer developing system countermeasures to prevent data intrusions from unauthorized users
Business Processes	**Healthcare**	A healthcare consultant to government and major healthcare entities in digital transformation of healthcare organizations
Cybersecurity Protocols	**Cybersecurity**	A zero trust compliance manager implementing measures to protect national security data
Human in the Loop	**Healthcare**	A hospital pharmacy director responsible for reviewing patient records with prescriptions; an emergency room physician with daily access to patient records;
User Awareness	**Healthcare**	A healthcare record manager expert with daily EHR interactions at a major healthcare provider, and responsible for maintaining the EHR in a major healthcare system
Regulations	**Policy**	A policy director from a government agency responsible for the development and compliance of cybersecurity policy to protect national security data.

Table 2: STS Factors and Subject Matter Experts (SMEs) for Semi-Structured Interviews

Table 3 includes the questions asked to the SMEs to inform the semi-structured interviews and qualitative data requirements for Essay 1.

Essay 1: Human Technology Interface Error in Healthcare Data Breaches		
Why Organizations Should Care About Cybersecurity?	What are the Most Common Situations Where Human Errors Have Led to Security Breaches?	What STS Factors Have the Most Impact Reducing the Risk of Human Errors?

Table 3: Essay 1 SMEs Interview Questions

<u>Quantitative Data –Clustering Analysis</u>

State healthcare systems are effective DMUs for Malmquist performance index analysis due to their structured inputs (number of managed patients, healthcare expenditures, etc.) and measurable outputs (lengths of hospital stay, deaths). These metrics enable

assessing how input resources are utilized to drive productivity and performance changes over time. Although state healthcare systems (DMUs) may exhibit heterogeneity, they still are comparable because they operate under the same federal regulatory framework. This standardization allows for meaningful benchmarking while still accounting for variations in operational productivity across different states.

A study sponsored by IBM Security, on the cost of a data breach, presents evidence that factors such as gross domestic product (GDP) and healthcare IT budgets can contribute to heterogeneity of DMUs (Ponemon Institute, 2022). Data variability is a central consideration in statistical analysis, as it can affect the perceived reliability of the data and the decision making process. One major challenge in performance benchmarking is the variation in economic and demographic factors across states.

Data by State	Category	Range	Source
Population	Demographics	1997-2022	Department of Commerce (DoC)- Census Bureau's American Community Survey (ACS)
GDP per Capita	Economics and Demographics	1997-2022	DoC- U.S. Bureau of Economic Analysis (BEA)
Healthcare Expenditure	Healthcare Economics	1991-2022	DHHS- Centers for Medicare & Medicaid Services, Office of the Actuary, National Health Statistics Group
Healthcare Expenditure as a % of GDP	Healthcare Economics and Demographics	1991-2022	DHHS- Centers for Medicare & Medicaid Services, Office of the Actuary, National Health Statistics Group
Patients' Health Insurance (Employer, Military, Medicaid, Uninsured)	Healthcare Services and Demographics	1999-2022	DoC- Census Bureau's American Community Survey (ACS)
Physicians and Clinical Services	Healthcare Services	1991-2020	DHHS- Centers for Medicare & Medicaid Services, Office of the Actuary, National Health Statistics Group
Hospitals by Type	Healthcare Services	1991-2020	American Hospital Association (AHA) Annual Survey
Hospital Admission per Capita	Healthcare Services and Demographics	1999-2022	American Hospital Association (AHA) Annual Survey
30 Day Hospital Readmissions	Healthcare Services	2020-2022	American Hospital Association (AHA) Annual Survey
Emergency Room Visits	Healthcare Services	1999-2022	American Hospital Association (AHA) Annual Survey
Hospital Inpatient Days	Healthcare Services	1999-2022	American Hospital Association (AHA) Annual Survey
Mortality Rate	Health Status	2000-2022	DHHS -Centers for Disease Control and Prevention's National Center for Health Statistics
Data Breach Incidents	Information Security	2009-2024	DHHS- Office of Civil Rights

Table 4: Quantitative Dataset of Contextual and Operational Variables Used in the Principal Component Analysis (PCA)

Clustering algorithms were applied to address the variability of the DMUs. The first step in the analysis consisted in assessing 13 contextual and operational variables. Multiple principal component analysis (PCA) iterations were performed to reduce the dimensionality of the dataset assembled (Greenacre et al., 2023). Table 4 illustrates the

contextual and operational variables used in the PCA analysis. PCA's results were then used with DBSCAN clustering algorithms to identify the optimal number of clusters.

Table 5 presents a structured template of the data fields that were assembled to support the PCA modeling and data analysis conducted to reduce the dimension of the dataset used for the clustering analysis.

DMU	Population	GDP by State per Capita	Health Spending	Healthcare Exp as % of GDP	People Insured	Healthcare Professionals	Hospitals	Hospital Admissions per Capita	30 Day Hospital Readmissions	Emergency Room Visits	Inpatient Days	Data Breach Incidents	Mortality Rate
Alabama	5,073,903	$ 54,754	$ 60,726,815	0.198	4,494,600	18,539	102	0.119	87,429	2,065,079	3,840,945	58	0.0127
Alaska	733,276	$ 86,759	$ 13,262,759	0.198	623,900	3,103	20	0.070	7,361	237,581	418,701	18	0.0082
Arizona	7,365,684	$ 62,309	$ 86,397,400	0.170	6,445,900	26,391	87	0.087	92,213	2,158,145	3,425,043	107	0.0103
Arkansas	3,046,404	$ 54,235	$ 37,627,676	0.211	2,701,500	12,085	93	0.115	51,605	1,447,042	1,934,467	63	0.0128
California	39,040,616	$ 92,163	$ 539,087,598	0.134	35,709,100	157,925	355	0.081	465,805	13,117,647	18,349,090	495	0.0082
Colorado	5,841,039	$ 82,926	$ 66,279,224	0.127	5,295,600	23,520	92	0.074	61,464	2,359,780	2,470,759	96	0.0082
Connecticut	3,608,706	$ 89,186	$ 59,067,474	0.161	3,325,900	24,689	31	0.100	54,167	1,602,265	2,251,833	93	0.0099
Delaware	1,019,459	$ 85,854	$ 16,924,477	0.168	936,100	4,369	8	0.100	14,436	433,270	698,329	20	0.0115
District of Columbia	671,803	$ 241,610	$ 13,629,728	0.071	620,000	9,730	10	0.161	16,083	361,430	875,359	21	0.0084

Table 5: Dataset Used in the PCA to Reduce the Dimensions for the Clustering Analysis

To address this variability in the DMUs and to create more homogeneous comparison groups, state population size, GDP, and healthcare spending data were analyzed using the data sources included in Table 6. When visualizing the data and testing multiple clustering algorithms, population size and GDP consistently provided as key differentiators, with some states showing patterns linked to larger populations and higher incomes. State GDP and population are strong measures for determining state healthcare system clusters because they capture both the economic capacity and demand for healthcare services of the DMU, which are critical factors influencing healthcare system performance. By considering both variables, DMUs can be grouped into clusters that reflect their ability to provide healthcare services relative to their demand. This heterogeneity, if not resolved, can particularly present major challenges for establishing accurate performance benchmarks.

Data by State	Category	Range	Source
Population	Demographics	1997-2022	Department of Commerce (DoC)- Census Bureau's American Community Survey (ACS)
Gross Domestic Product (GDP)	Economics	1997-2022	DoC- U.S. Bureau of Economic Analysis (BEA)
Healthcare Expenditure per Capita	Healthcare Economics and Demographics	1991-2022	DHHS- Centers for Medicare & Medicaid Services, Office of the Actuary, National Health Statistics Group

Table 6: Quantitative Datasets with Sources and Data Range Used for Clustering Analysis

A K-Means algorithm with three clusters was applied, using state GDP and population as the primary factors for segmentation. K-Means was selected due to its simplicity and because is particularly well-suited for grouping data into distinct, non-overlapping clusters, mitigating heterogeneity and reducing bias in modeling and hypothesis testing (Yadav et al., 2013).

Table 7 shows the DMUs, defined as the state healthcare systems, grouped into three relatively homogeneous clusters: high-capacity; mid-capacity; and low-capacity states. A valuable direction for future research shall include breaking it up low-capacity states into two or more sub-groups to create more homogeneous comparison groups. This segmentation can improve the precision and fairness of productivity benchmarking and the regression models by reducing variability within groups, allowing for more meaningful peer comparisons and targeted policy insights for similarly constrained healthcare systems.

Cluster 1: High-Capacity States	Cluster 2: Mid-Capacity States	Cluster 3: Low-Capacity States		
California	Florida	Alabama	Kentucky	Oklahoma
New York	Georgia	Alaska	Louisiana	Oregon
Texas	Illinois	Arizona	Maine	Rhode Island
	Massachusetts	Arkansas	Maryland	South Carolina
	Michigan	Colorado	Minnesota	South Dakota
	New Jersey	Connecticut	Mississippi	Tennessee
	North Carolina	Delaware	Missouri	Utah
	Ohio	District of Columbia	Montana	Vermont
	Pennsylvania	Hawaii	Nebraska	West Virginia
	Virginia	Idaho	Nevada	Wisconsin
	Washington	Indiana	New Hampshire	Wyoming
		Iowa	New Mexico	
		Kansas	North Dakota	

Table 7: States Organized by High-Capacity, Mid-Capacity, and Low-Capacity Clusters

Quantitative Data Collection

A comprehensive quantitative dataset of real-world healthcare IT data supports the hypothesis testing and the findings presented in Chapter 2 (Essay 1), Chapter 3 (Essay 2), and Chapter 4 (Essay 3). This dataset includes all reported cybersecurity incidents and compromised patient records from DMUs submitted to the DHHS OCR, as mandated by the HIPAA Privacy and Security Rules since 2009. It encompasses data

breach incidents reported by healthcare organizations across all 50 states and the District of Columbia (HIPPA, 2024).

Data by State	Category	Range	Source
Hospital Adoption of EHRs	Business Process Modernization	2009-2020	DHHS -Centers for Disease Control and Prevention's National Center for Health Statistics
Healthcare Nursing Facilities Adoption of EHRs	Business Process Modernization	2009-2019	DHHS -Centers for Disease Control and Prevention's National Center for Health Statistics
Data Breach Incidents	Information Security	2009-2024	DHHS- Office of Civil Rights
Patient Records Compromised	Information Security	2009-2024	DHHS- Office of Civil Rights

Table 8: Quantitative Datasets with Sources and Data Range for Essay 1

The datasets presented in Table 8 consists of breach incident reports from healthcare entities, including hospitals, health insurance plans, business associates, and healthcare clearinghouses. It captures cybersecurity incidents with daily reports spanning from 2009 to 2024. The dataset comprises eight key fields: the name of the breached entity, covered entity type, breach submission date, year, state, number of affected records, type of breach, and location of the breached information. The data also includes EHR adoptions at hospitals and healthcare nursing facilities.

Table 9 presents a structured template of these dataset fields, which were assembled to support the modeling, hypothesis testing, and data analysis conducted in this dissertation. In total, the dataset includes 6,594 reported healthcare data breach incidents from 2009 to 2024, each involving 500 or more compromised records.

Name of Entity Breached	Cover Entity Type	Breach Submission Date	Year	State	Records Affected	Type of Breach	Location of Breached Information
CHCM, Inc. dba College Hospital Costa Mesa	Healthcare Provider	12/18/2024	2024	California	22,171	Hacking/IT Incident	Network Server
Ott Cone & Redpath, P.A.	Business Associate	11/18/2023	2023	North Carolina	13,000	Loss	Email
California Correctional Health Care Services	Healthcare Provider	1/18/2010	2010	California	97,488	Unauthorized Access/Disclosure	Paper Films
SAG-AFTRA Health Plan	Health Plan	2/18/2015	2015	California	500,000	Theft	Desktop Computer

Table 9: Quantitative Datasets of Breach Incidents Reported by U.S. Healthcare Entities

To conduct the assessment of the dataset retrieved from the DHHS OCR, a Microsoft Excel database was created to log all data breach incidents. This database served as a management and analysis tool, facilitating the selection of data fields for the research. Given the large volume of data, Excel pivot tables were incorporated to categorize and

accurately quantify the events based on multiple fields, and criteria requirements for analisis of results.

Data collected from 2009 to 2024 were categorized based on the number of breaches, the volume of compromised patient records, and the specific locations within healthcare IT systems where these breaches occurred. These locations include emails, network servers, paper or film records, digital records, laptops, desktop computers, portable electronic devices, and other storage points. After analyzing and visualizing the data, breach events were quantified to assess the impact of human error on healthcare data breaches and to determine the relative importance of breach locations within IT systems of the DMUs.

2.4.2 Approach - Literature Review

This chapter uses the results of a systematic literature review to explore the application of STS factors influencing human error in data breaches of EHR. The literature review was informed by articles from various datasets and web-based resources. Ten keywords (Computer Security, Cybersecurity, Data Breaches, Data Envelopment Analysis, Electronic Health Records, Healthcare, Human Error, Methods, Risk, and Socio-Technical Systems) were used to retrieve 1,071 documents, which were then screened to identify relevant publications. In line with the systematic review guidance from Transfield (Transfield et al., 2003), Sardi and Rizzi (Sardi et al., 2020), Snyder (Snyder, 2019), and Katharakisa (Katharakisa et al., 2013), 40 articles were selected from the initial 1,071 sources (Alvarado, Triantis, 2024).

Literature reviews are an important aspect and critical step for conducting research. They provide the basis for developing the foundational background in the specific area of research, and necessary to justify the research questions, and hypotheses. Based on the literature information from Snyder 2019, three types of literature review approaches were evaluated: systematic; semi-systematic; and, integrative approaches; for selecting the “best fit” approach to generate this research paper (Snyder, 2019). After evaluating these methodologies, the systematic literature review was determined to be the most suitable approach for analyzing the selected publications (Alvarado, Triantis, 2024).

Systematic reviews have been broadly used in medical and healthcare related research, and have been referred to as the “gold standard” among reviews (Davis et al., 2014). This approach was selected because the goal of this study was to identify all empirical evidence, while minimizing bias or speculations based on expert knowledge in the field or common beliefs about what is generally accepted, and to identify the most impactful findings from which results and recommendations about the STS factors influencing human error in data breaches and EHR adoption and information sharing can be reached (Armitage et al., 2009) (Snyder, 2019).

Although there are many approaches to carry out a systematic review, the Transfield approach was adopted (Transfield et al., 2003) because it is one of the most recognized in the management literature, with more than 8,000 citations on Google Scholar and Web of Science, and has been tested and validated by the research community (Sardi, 2020). The approach (adapted from Transfield) suggests the following steps for conducting a rigorous review: planning the literature review; conducting a review; extracting the relevant documents; and, validating the reports (Alvarado, Triantis, 2024).

.

Planning the literature review: Eleven previously published healthcare journal papers informed the literature review. Three of these papers, authored by information security experts, addressed cyber risks and human factors in healthcare systems (Sardi et al., 2020), (Nifakos et al., 2021) (Franke et al., 2014). Another five focused on measuring productivity and tackling managerial challenges within healthcare systems (Liberati et al., 2009) (Davis et al., 2014) (Katharakisa et al., 2013) (Crema et al., 2013) (Menear et al., 2014). To guide the review process, three additional journal papers on systematic literature review methodologies were consulted (Armitage et al., 2009) (Tranfield et al., 2003) (Keathley-Herring et al., 2016).

Additionally, insights were gathered through consultations with a healthcare professional specializing in EHR data mining tools and multiple interviews with cybersecurity experts responsible for protecting national defense networks from cyber intrusions. These discussions provided valuable perspectives on system vulnerabilities

and human-technology interactions in healthcare information security. Drawing from the literature and expert insights, key search terms and the keywords were used for sourcing relevant publications, as outlined in Table 10 (Alvarado, Triantis, 2024).

	Keywords				
	Computer Security	***Cybersecurity***	***Data Breaches***	***Data Envelopment Analysis***	***Electronic Health Records***
Linked Keywords	Cyber Security	Cyber Risks	Data Breaches	Hospital Efficiency	Electronic Health Records
	Ethics	Cyber Attacks	Redundancy	E-Health	Patients Health Information
	Network Security	Zero Trust Architecture	Healthcare	Efficiency	HIPAA Policy
	Computer Science	Identity Access Management	Information Security Policy	Health IT	Electronic Medical Records
	Healthcare	***Human Errors***	***Methods***	***Risk***	***Social Technical Systems***
Linked Keywords	Health	Human Errors	Literature Review	Risk Management	System Thinking
	Healthcare Sector	Internal Threat	Resiliency	Risk Assessment	Socio Technical Theory
	Healthcare Facilities	User Awareness	Framework	Risk Evaluation	Accident Analysis
	Medical IT	Human Mistakes	Reliability Theory		System Dynamics
	Security of Health Data		Control Theory		Human Relations
			Economic Production		Organizational Change
					Safety Incidents

Table 10: Keywords Used to Search Publications for the Literature Review

Conducting the review: The literature review incorporated information from various electronic search engines, including Google Scholar, as well as electronic libraries from the National Institute of Health (NIH), Virginia Polytechnic Institute and State University, the University of Southern California, and George Mason University. Additional sources included industry reports and company websites, federal government publications from the Department of Commerce's National Institute of Standards and Technology (NIST) and the Department of Health and Human Services (DHHS), and statistical data on healthcare data breaches from the HIPAA Journal (Alvarado, Triantis, 2024).

To ensure a comprehensive review, articles from medical science magazines were also examined, offering diverse perspectives from healthcare experts. The literature sources encompassed peer-reviewed journals and university research papers from a range of databases, including Academic Press, the American Medical Association, CrossMark, De Gruyter, Scopus Elsevier, the Institute of Electrical and Electronics Engineers (IEEE), NIH, Journal Storage (JSTOR), Oxford University Press, Research Gate, Springer, and the Taylor & Francis Group, among others (Alvarado, Triantis, 2024).

To conduct the assessment and synthesis of the documents retrieved from the literature, a Microsoft Excel spreadsheet was created to log all 1,071 documents from

the initial search. This spreadsheet served as a management and analysis tool, facilitating the selection of relevant publications for the research. Given the large volume of documents, Excel pivot tables were incorporated to categorize and accurately quantify the documents based on multiple criteria, including publication trends (Alvarado, Triantis, 2024).

The next section presents the literature findings by publication trends. Table 11 classifies all retrieved publications by subject area and associated keywords, while Table 12 categorizes the documents by type, such as journals and research papers, based on keyword relevance (Alvarado, Triantis, 2024).

.

	Keywords										
Subject Area	Computer Security	Cybersecurity	Data Breaches	DEA	EHRs	Healthcare	Human Errors	Methods	Risk	STS	Total
Communications	37	0	3	0	6	0	10	0	1	6	63
Economics	0	0	2	0	0	2	0	1	0	0	5
History	0	0	0	0	0	4	0	0	0	0	4
Human and Social Factors	6	11	12	9	75	96	23	7	21	33	293
Information Systems	37	99	43	0	50	26	22	7	1	10	295
Management Science	6	4	22	0	8	10	6	10	3	8	77
Modeling	3	5	5	0	9	9	6	2	0	9	48
Operations	6	3	6	0	2	2	12	0	1	9	41
Safety and Risk Analysis	1	12	5	0	8	2	12	4	18	8	70
Science	38	0	0	0	0	5	1	0	3	0	47
Technology & Engineering	5	2	0	0	0	1	13	1	3	11	36
Theory and Policy	8	17	26	0	3	3	1	22	2	10	92
Total	147	153	124	9	161	160	106	54	53	104	1071

Table 11: Publications' Trend-By Keywords and Subject Area

	Keywords										
Document Type	Computer Security	Cybersecurity	Data Breaches	DEA	EHRs	Healthcare	Human Errors	Methods	Risk	STS	Total
Articles	5	13	5		7	66	2	5	18	1	122
Books / Handbooks	6	14	3			18	3	6	1	9	60
Doctoral Theses	2	4	1	1	1			1		2	12
Journals	104	34	71	6	110	37	90	15	11	84	562
Notes and Links	1	1				1					3
Research Papers	29	87	44	2	43	38	11	27	23	8	312
Total	147	153	124	9	161	160	106	54	53	104	1071

Table 12: Publications' Trend By Keywords and Document Type

Extracting the relevant documents: Once all documents were retrieved from multiple data sources and categorized by year and by publication type, the inclusion and exclusion criteria included in Table 13 were applied to determine which papers were incorporated into the literature review (Alvarado, Triantis, 2024).

.

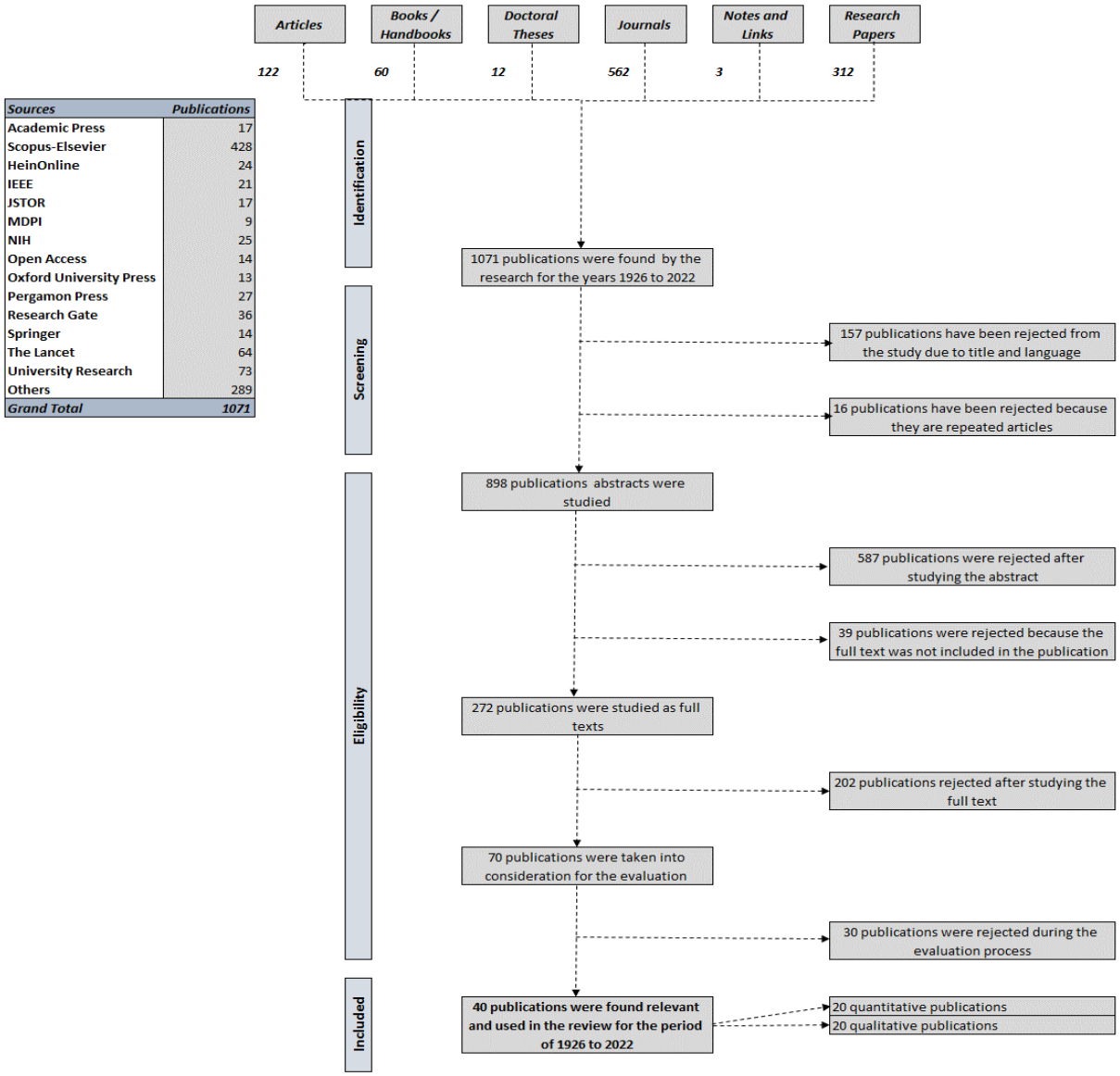
Inclusion Criteria	Exclusion Criteria
Publications relevant to cyber security threats to the healthcare sector	Duplicates and repeated publications
Articles that report on STS factors associated with cyber security management	Articles that by their titles were found irrelevant to the research questions or hypotheses
Articles that report on data breaches occurring in hospitals and other healthcare organizations	Documents that were not written in English
Publications that report human, technical, and organizational factors that drive human error in the healthcare sector	Publications that were not related nor had any implications to the healthcare sector environment
Publications that address barriers and solutions for EHR adoption and information sharing	Articles that were focused primarily on technical developments (e.g., algorithms, software) and failed to address their implications to data breaches, EHR, or involvement of human in the loop-healthcare professionals
Articles that identify vulnerabilities of the healthcare information technology infrastructure	
Publications relevant to policy and system capabilities aimed at protecting patients' PHI	

Table 13: Criteria Used for Selecting Relevant Documents to Inform the Dissertation

First, 157 publications were removed because they were not written in English or because the title of the document was found irrelevant to the questions and hypotheses of this study. Second, 16 documents that were duplicates or repeated were rejected. After studying the abstract of the remaining 898 documents and based on the inclusion and exclusion criteria, 626 articles that were not related to data breaches were rejected, or did not have any implications for the healthcare sector environment, or were incomplete (Alvarado, Triantis, 2024).

The review of the document abstracts enabled elimination of documents that were published prior to the introduction of the 1996 HIPAA Privacy Protection Act as they were found to be out of date and irrelevant to the aim of the paper. Consequently, 272 publications were selected for studying the full text. In the next step, I read the full text of these 272 publications and selected 70 documents useful to inform the aim of the study. Finally, after conducting an in-depth evaluation of the 70 documents, only 40 publications were selected. This final selection was limited to articles that specifically addressed the three main aspects of this study: STS factors influencing human error in

data breaches and EHR adoption. Figure 7 illustrates a flow chart of the process used for the selection of these articles (Alvarado, Triantis, 2024).



Sources	Publications
Academic Press	17
Scopus-Elsevier	428
HeinOnline	24
IEEE	21
JSTOR	17
MDPI	9
NIH	25
Open Access	14
Oxford University Press	13
Pergamon Press	27
Research Gate	36
Springer	14
The Lancet	64
University Research	73
Others	289
Grand Total	*1071*

Figure 7: Flow Chart of the Process Selection of Relevant Documents

Quantitative publications were based on empirical observations where analytical quantitative evaluations, including statistical analysis of historical data and testing of hypotheses, were presented. Meanwhile, qualitative publications were based on methods where the authors conducted surveys and developed conceptual models to influence future research and policy development (Alvarado, Triantis, 2024).

Validating the results: The findings were examined and a taxonomy of human error causing data breach incidents, and a conceptual framework of the STS factors that drive human error in data breaches were developed. The inclusion criteria provided the basis for the literature search where the “human error on data breaches” within the title, abstract, and body of the publications were used to select the relevant documents for the study. This approach provided a solid foundation for filtering out unrelated studies, aligning the selected document with the research objective. Information systems, human and social factors, safety and risk analysis, and management science were the key focus subject areas to relate the publications to data breaches and data privacy in healthcare from a management perspective. (Alvarado, Triantis, 2024).

The document exclusion criteria ensured current reality of what is happening in the dynamic information security environment and the implications that protection of data privacy is having in the adoption and information sharing of EHR. For example after reviewing the abstracts, publications predating 1996 were excluded, as they did not reflect the impact of major regulatory changes, such as the introduction of HIPAA’s privacy protection measures, or the technological advancements that reshaped healthcare data management. Additionally, sources such as blogs, magazines, unreliable websites, and newspapers were disregarded to maintain academic rigor and ensure the credibility of the reviewed literature (Alvarado, Triantis, 2024).

Two conceptual frameworks were derived from the literature: one being the taxonomy of human errors causing data breach incidents, and the other a management framework based on STS principles. These frameworks are presented and further explained in the results section, Figures 11 and 12. Essay 1 uses these frameworks to assess the significance of the location where human error-related data breaches occur and their severity on patient record privacy. The hypothesis in this essay states that:

> **H1: The location where data are breached within healthcare IT systems, as a consequence of errors from the human-technology interface, significantly influence the severity of data breaches impacting the security and privacy of patient records.**

To test the hypothesis, the data were analyzed and visualized, quantifying breach events to assess the impact of human error on healthcare data breaches. This analysis identified the relative importance of breach locations within the IT systems of the DMUs.

2.5 Results and Discussion

Qualitative Results - Semi-Structured Interviews

Semi-structured interviews provided valuable insights from cybersecurity and healthcare professionals on nuances in patient care practices that were not evident in the literature. When structured properly, these interviews enhance the depth and credibility of the dissertation by incorporating real-world experiences into the research. Appendices F thru J include the semi-structured interview protocols with interview questions and structure followed, list of SMEs and their associated expertise by STS factor, responses to questions, summary of results, and the Virginia Tech Institution Review Board (IRB) request and approval forms.

The Table 14 included below provides a summary of the findings from the semi-structured interviews, including takeaways, qualitative results, and how the findings inform Essay 1 hypothesis and research question.

Literature Gap	Interviews Takeaway	Interview Findings	Qualitative Results	How Findings Inform the Research
Essay 1: Impact of STS factors on human-technology interaction errors	Protection of data should be highest priority	Importance of reducing human error • Protection of data should be highest priority • Keeping patient trust • Reduce legal implications • Impact to business base Most common locations where data are breached • Data transfers • Password hygiene • System application vulnerabilities • Social engineering Most impactful STS to occurrence of human error • Identity access management (IAM) • System diversity • User awareness • Human in the loop	Provided insight into most common human errors and sources and locations where data are breached	Location where data are breached • Data transfers: Emails, paper films, EHR • PW hygiene: Network servers, desktop computers • System vulnerabilities: Network servers • Social engineering: Network servers, emails

Table 14: Essay 1 Results from Semi-Structured Interviews and How the Findings Inform the Research Study

The interviews provided additional insights into the impact of data breaches to the organizations and highlighted the following findings for Essay 1: human error data breaches affect healthcare provider's business decisions; data transfers and password hygiene emerged as the most common human errors contributing to data breaches; and emails and access to network servers are the most common locations where data are breached.

Quantitative Results

Figure 8 illustrates that between 2009 and 2024, a total of 6,594 healthcare data breaches involving 500 or more records were reported. The data also show that human errors, directly or indirectly, are responsible for 84% of these breaches and 95% of all compromised patient records. The data breach event graph (left plot) presents the ascending trend that the healthcare sector has experienced since the first reporting date in 2009. This trend confirms the challenge that the healthcare sector is facing to protect its data, as the sector has become a victim of external and internal cybersecurity attacks. Additionally, as organizations increasingly rely on digital solutions to enhance their services, the financial burden of data breaches is expected to remain a pressing concern.

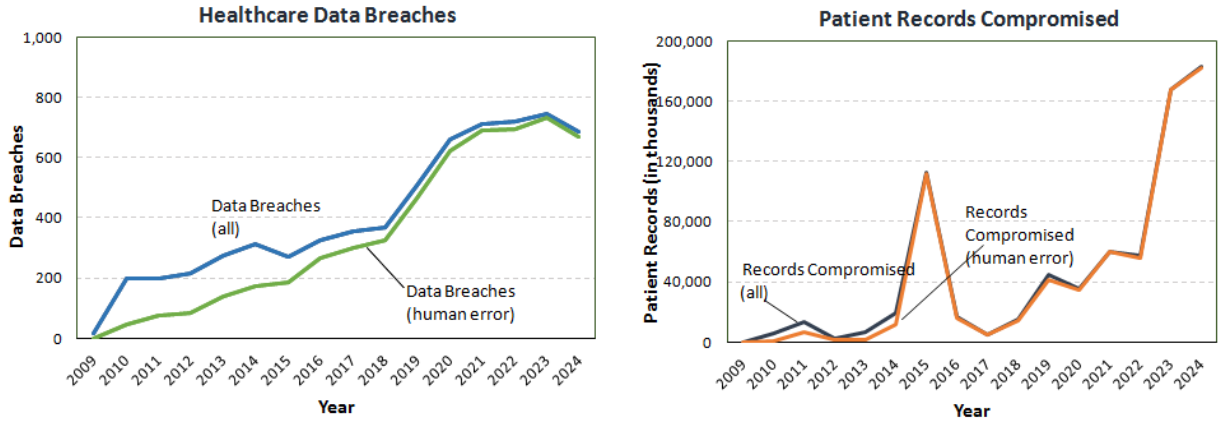
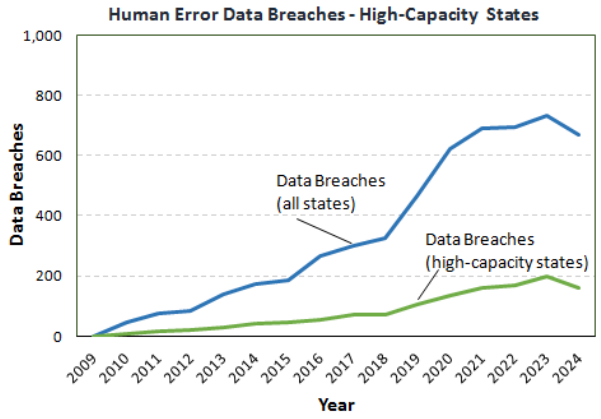


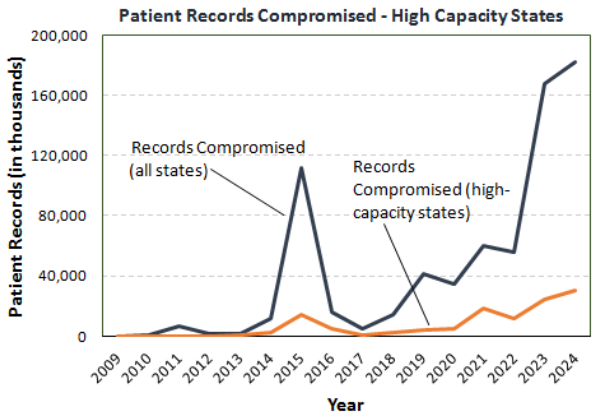
Figure 8: Historical Trend by Year of Healthcare Data Breaches and Patient Records Affected by All States (HIPAA, 2024)

The compromised patient records graph (right plot) shows that data breaches resulted in the loss, theft, exposure, or impermissible disclosure of 741,340,196 records (HIPPA,

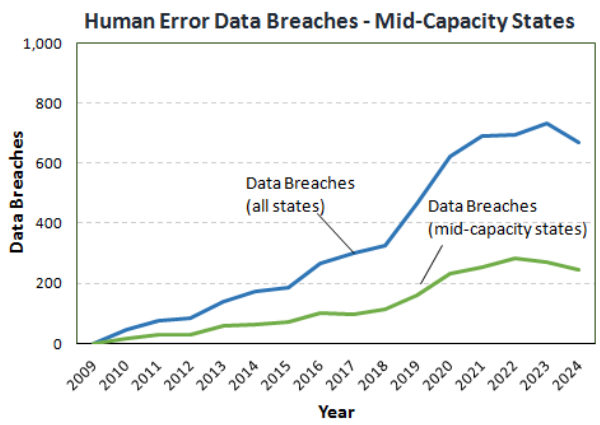
2024). The plot also highlights a significant event in 2015 when the healthcare sector experienced its largest recorded data breach. Anthem Inc., based in Indianapolis, IN, suffered the largest ever healthcare data breach recorded affecting 78.8 million records. The incident resulted in approximately $400 million in total costs, including remediation expenses, lawsuit settlements, penalties from state attorneys general, and the resolution of the DHHS OCR investigation (HIPAA, 2022). As indicated by the trend, the protection and security of patients' PHI from human error-related data breaches remains a persistent challenge for the healthcare industry in advancing EHR adoption (Tran, 2021).

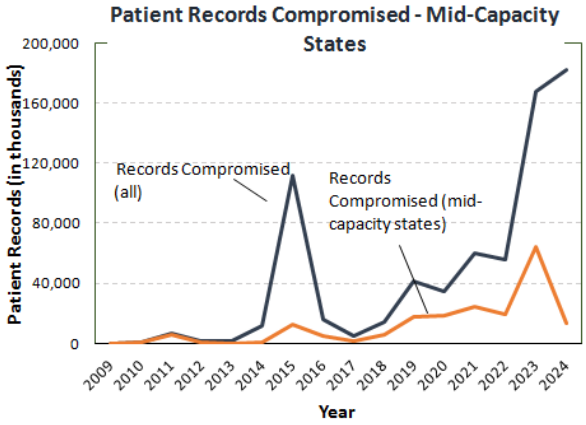
Figure 9 illustrates that the average trends in data breaches and the number of compromised records show the variability across the three state clusters, a pattern that has remained consistent from 2009 to 2024. These clusters, high-capacity, mid-capacity, and low-capacity states, were established through the clustering analysis described in a previous section of this chapter. As expected, the highest averages are observed in high-capacity, highly populated states such as California, New York, and Texas, where a greater volume of patient records are exposed. Particularly, apart from the Anthem Inc. unprecedented data breach, occurring in the low-capacity state cluster, the trend in data breaches for high-capacity and mid-capacity states aligns with the number of records compromised within these clusters.



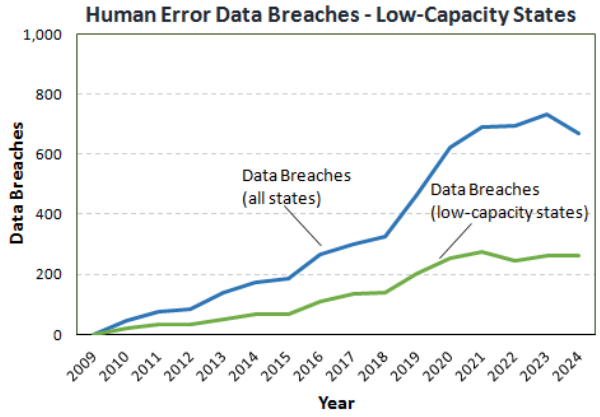


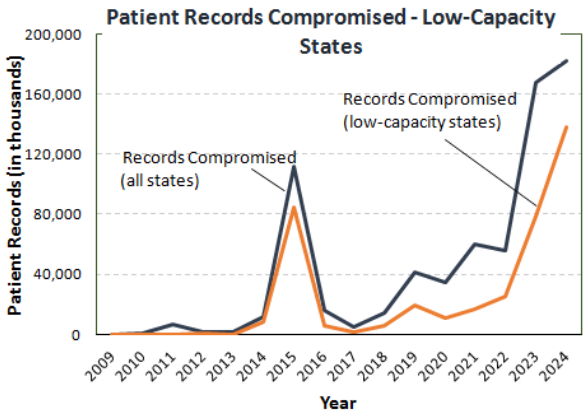
Year (High-Capacity States)	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Avg Data Breaches	0	3	5	6	10	14	16	18	23	24	35	45	54	56	67	53
Avg Compromised Records	0	23	27	29	252	950	4,754	1,611	404	937	1,378	1,718	6,096	3,892	8,238	10,158





Year (Mid-Capacity States)	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Avg Data Breaches	0	1	3	3	5	6	7	9	9	10	14	21	23	26	25	22
Avg Compromised Records	0	79	555	51	29	51	1,173	461	167	557	1,643	1,666	2,254	1,759	5,861	1,248





Year (Low-Capacity States)	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Avg Data Breaches	0	1	1	1	1	2	2	3	4	4	5	7	7	7	7	7
Avg Compromised Records	0	4	9	32	7	221	2285	160	53	151	529	296	460	679	2133	3749

Figure 9: Trend of Human Error Data Breaches and Patient Records by High-Capacity, Mid-Capacity, and Low-Capacity State Groups (HIPAA, 2024)

Figure 10 reveals that healthcare providers account for the majority of data breaches and compromised records. These incidents are also significantly higher for high-capacity states compared to mid-capacity and low-capacity states. This trend is not a surprise, as healthcare providers have the largest workforce and the highest number of digital devices accessing EHR data (HIPAA, 2022).

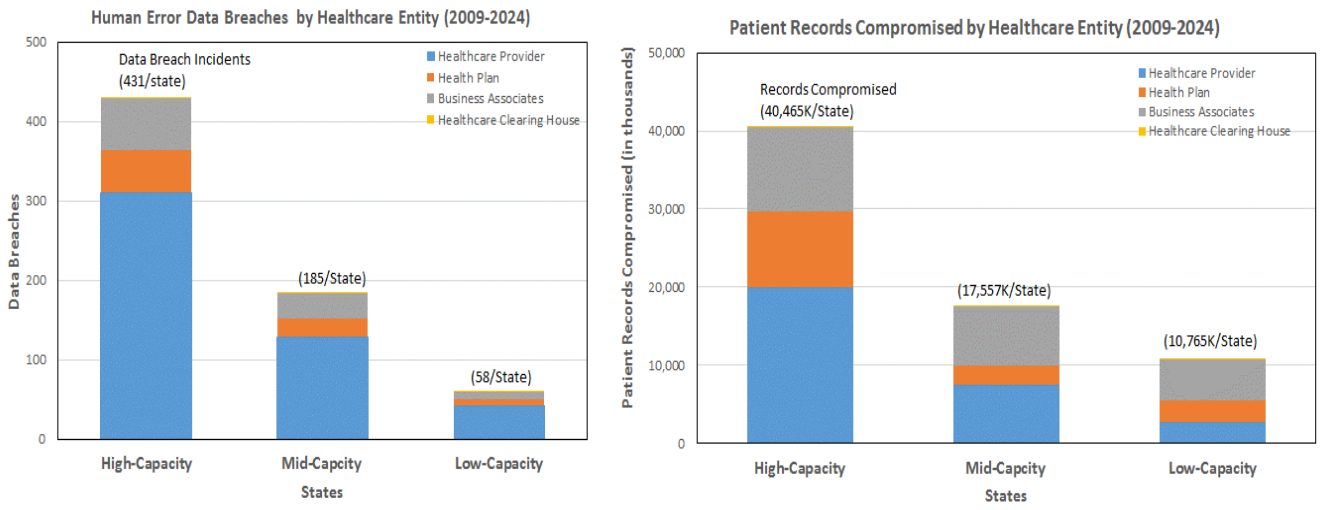


Figure 10: Data Breach Incidents and Compromised Patient Records by Healthcare Entity Where They Originated (HIPAA, 2024)

Taxonomy of Human Error Causing Data Breach Incidents - Representation of Reason's Persons Approach (Reason, 2000).

One objective in this essay was to review relevant literature in information security to understand and analyze sources of error and people's motivation leading to human error causing data breaches in the healthcare sector. To accomplish this objective, causes of human error and the locations where data are breached were analyzed to develop a taxonomy of human driven privacy data breach incidents.

To contextualize this taxonomy, Figure 11 categorizes all human errors based on three common causes of error identified in information security:

- ***Unintentional errors:*** are caused due to the lack of knowledge or skills, or simply a distraction (Lahcen et al., 2020).

- ***Intentional errors:*** could be the result of an employee's reckless behavior who knows of potential risk but is careless (Parsons et al., 2017) and (Ahola, 2020).

- ***Malicious errors:*** are caused when the behavior of the employee is intentional and can have major damaging consequences (Liginlal et al., 2008).

The findings from this taxonomy offer information security practitioners a solid base of the sources of human error within the IT systems to enable design of more resilient systems.

Human Error Type	*Source of Human Error Causing Data Breaches*
Unintentional -- ***Lack of knowledge or skill, distraction***	Data entry error
	Lack of/or incorrectly recording privacy policy agreement
	Leaving sensitive information accessible to others
	Inappropriate skill in IT SW
	SW vulnerabilities
	Improper disposal of information
	Lost/misplaced mobile devices
	Lost paperworks
	Work pressure (pressure to work too fast)
	Employee attitude and behavior
	Insufficiently protecting stored information (e.g. encryption)
	Lack or improperly documented procedures
	Stress
	Not following security best practices
	System design flaws
	Loss of confidential security and credential
	Email misdelivery- releasing information to the wrong person
	Lack of awareness and training
	Lack of supervision
	Down loading internet files from unknown sources
	Victim of phishing
	Password hygiene
Intentional-- ***Know of potential risk but reckless***	Collecting information beyond requirement or unrelated to the purpose
	Restricting owners' access to information
	Storing or handling information in unsecured manner for the sake of simplicity or efficiency
	Secondary use of information during processing
	Inserting removable unauthorized media
	Sending unencrypted data
	Releasing information to an unauthorized party
	Mishandling passwords
	Poor access control
	Insufficient monitoring
	Inadequate, incomplete, or delayed patching SW security vulnerability
Malicious-- ***Intentional and damaging consequences***	Unauthorized access
	Service disruption
	Malware infection
	Employee manipulation and malfeasance
	Posting PHI on social media
	Discussing PHI with third parties

Figure 11: Taxonomy of Human Driven Privacy Data Breach Incidents

<u>STS Management Framework to Human Error Challenge in Healthcare - Representation of Reason's Systems Approach.</u>

The literature identified a gap and the need for further research to investigate the impact of STS factors in reducing human error in information security. To address this gap, Figure 12 presents a conceptual framework of STS factors influencing human error that was developed to illustrate the role of STS in the information security landscape and the improvements needed to reduce errors. This framework emphasizes that the study of

complex systems, such as EHR, should account for the interactions and relationships between technology, organizational processes, people, and government policies.

EHR are complex systems due to their interrelationship with technical, regulatory, organizational, and human factors. From the technical standpoint, EHR need to communicate across multiple platforms, hospitals, clinics, and external organizations, often with incompatibles data formats and standards. EHR also must comply with strict regulations such as HIPAA, requiring strong security measures and patient data protection protocols. Organizationally, healthcare providers often resist EHR adoption and data sharing due to workflow disruptions, usability concerns, cost, and steep users' learning curves. Additionally, poorly designed EHR interfaces contribute to physician burnout, medical errors with life threatening consequences, and overall healthcare inefficiencies. Furthermore, healthcare professionals must also undergo extensive training to use EHR effectively, which adds to workload burdens. Addressing these complexities requires a STS thinking approach, integrating technological, human, organizational, and government regulatory considerations to enhance EHR effectiveness and usability.

An overview of the STS management factors is presented below.

- ***IAM Capabilities*** - Continual improvements in the design of IAM capabilities are essential for eliminating human-technology interface vulnerabilities in information security system (Megas et al., 2015). While healthcare systems have digitized to support EHR adoption and information sharing, the sector has not dynamically implemented trusted digital IAM solutions at the same pace, resulting in vulnerabilities within the records system.

- ***System Diversity*** - Implementing standardized IAM capability frameworks in healthcare systems that leverages common best practices and access controls, can help minimize human-technology interface errors (Jalali et al., 2018). The vulnerability of EHR systems in the U.S. healthcare sector is influenced by the weaknesses of individual healthcare units. In such a large and interconnected

system, reducing variability in IAM capabilities across healthcare units can enhance overall system security and resilience.

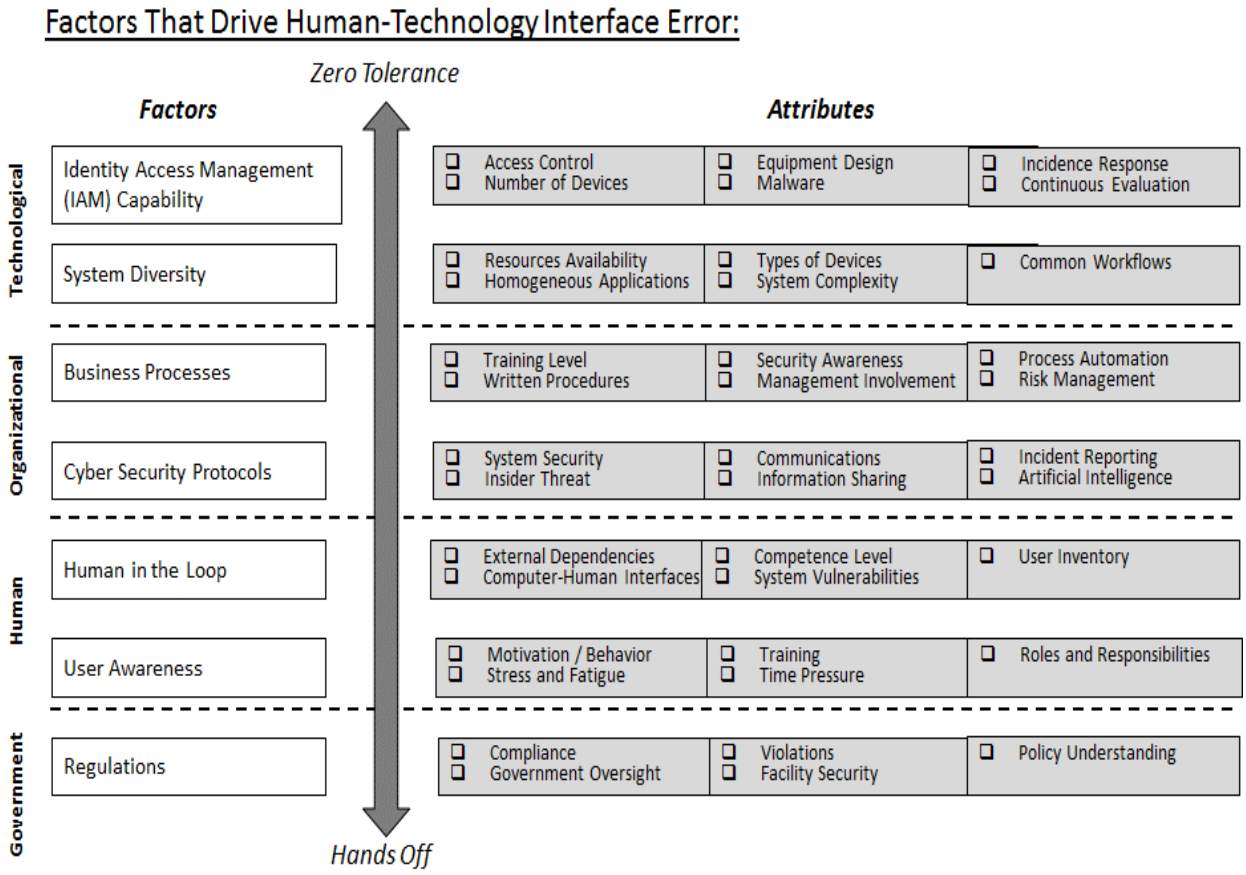


Figure 12: STS Management Framework of Factors That Drive Human-Technology Interface Error

- ***Business Processes*** **-** Organizations should prioritize raising employee awareness about human error and its role in data breaches (Miller et al., 2004). Given the sensitivity of patient information, healthcare management should foster a security-focused organizational culture where employees feel responsible for promptly reporting mistakes or unintentional disclosures of patient data without fear of repercussions (Hung, 2010).

- ***Cyber Security Protocols*** **-** Emphasizing the adoption of zero trust principles and tools to eliminate human error vulnerabilities can help establish a more defensible security architecture (Rose et al., 2020). Failure to follow cybersecurity protocols, such as neglecting two-factor authentication, increases

the risk of unauthorized access, making it easier for cybercriminals to infiltrate secure systems.

- ***Human in the Loop -*** Integration of healthcare stakeholders in the design of safeguards can help reduce human-technology interface errors. From an economic perspective, human error remains the leading cause of economic and productivity losses in the information systems security domain (Zimmerman et al., 2019).

- ***User Awareness*** - Identifying the causes of undesirable user behavior is essential for designing effective security systems (Safa et al., 2015). Additionally, raising awareness about the damaging consequences of cybersecurity incidents is crucial for ensuring that employees remain security-conscious while performing their daily tasks (Di Nella et al., 2021).

- ***Government Regulations -*** A combined approach of government oversight and industry actions can help prevent human error and mitigate risks associated with EHR use (HIPAA, 2022). Government oversight, through policy regulation, is essential for enforcing healthcare compliance with PHI security standards, reducing information security issues resulting from unintended consequences of EHR use (Bowman, 2013).

The Human Error Socio-Technical Systems (STS) Management Framework illustrated in Figure 12 is considered broadly applicable across a wide range of research and engineering fields involving human interaction with complex systems. Notable areas of relevance include human factors and ergonomics, aerospace and aviation safety, manufacturing engineering, transportation, human-robot interaction, and chemical process industries, among others.

Location in the Healthcare IT System Where Data are Breached as a Result of Human Error: Relative Importance to the Number of Compromised Patient Records.

The occurrence of data breaches from human error varies significantly by location. As shown in Figure 13 and Table 15, data breaches on network servers were the most

frequent and led to the highest number of compromised patient records. Human error-related data breaches involving emails were the second most common, contributing to six percent of all reported compromised patient records. Together, network servers and emails were responsible for 95 percent of the 713 million compromised patient records due to human-technology interface errors. Other breach locations, such as electronic medical records, paper/film records, portable electronic devices, and desktop computers, exhibited fewer incidents and had a smaller impact on the number of records compromised during the period from 2009 to 2024.

The data in Figure 13 indicates that the relationship between human error data breaches and the number of compromised patient records is not directly proportional. In other words, a higher frequency of data breaches in a specific location does not necessarily correspond to a greater number of compromised patient records.

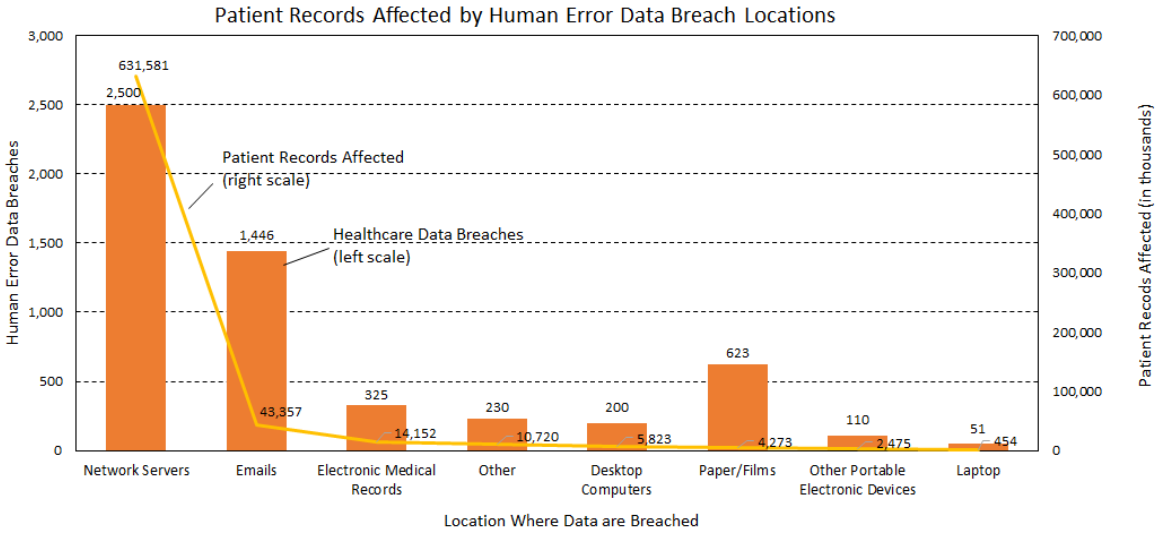


Figure 13: Locations Where Data Breaches Happened and Relative Importance to the Number of Compromised Patient Records (HIPAA, 2024)

State Groups (2009-2024)	Data Breaches				Patient Records Compromised (in thousands)			
Location Where Data are Breached	***High-Capacity***	***Mid-Capacity***	***Low-Capacity***	***Total***	***High-Capacity***	***Mid-Capacity***	***Low-Capacity***	***Total***
Network Services	622	943	935	2,500	104,230	165,030	362,320	631,581
Emails	325	530	591	1,446	9,871	13,705	19,782	43,357
Electronic Medical Records	77	115	133	325	485	4,357	9,311	14,152
Other	61	79	90	230	2,769	7,130	822	10,720
Desktop Computer	43	73	84	200	3,047	1,017	1,758	5,823
Paper/Films	125	226	272	623	807	1,637	1,829	4,273
Other Portable Electronic Device	29	43	38	110	117	165	2,193	2,475
Laptop	11	21	19	51	69	85	300	454
Total	***1,293***	***2,030***	***2,162***	***5,485***	***121,396***	***193,125***	***398,315***	***712,835***

Table 15: Locations Where Data are Breached and Compromised Patient Records by State Clusters

Data breaches on network servers occurred most frequently than any other location within healthcare IT systems. In this chapter, the location of where data breaches happened is assessed to determine the relative importance of these locations and provide insight to aid healthcare organizations in their prioritization of data protection measures. Figure 14 illustrates that the location vary significantly by state clusters. In general network servers were the main target followed by emails and paper/films, respectively.

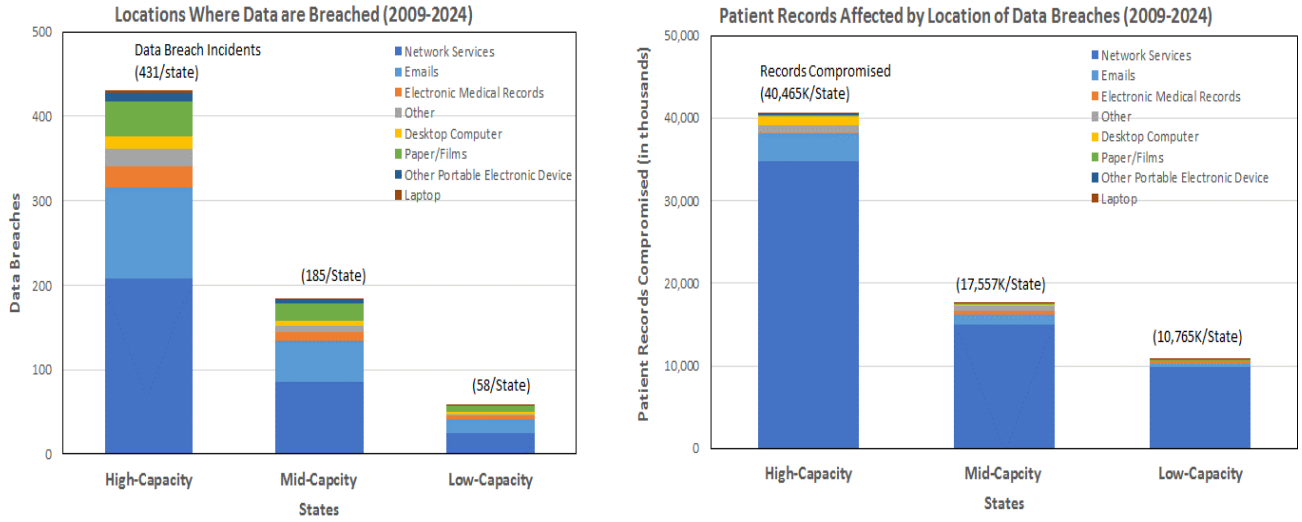


Figure 14: Data Breaches and Patient Records by Location Where Data Breaches Happened (HIPAA, 2024)

The analysis of data breach incidents, their locations, and the resulting compromised patient records offers valuable insights into the critical role of human factors in protecting EHR integrity. Figure 11, which presents the Taxonomy of Human Error Root

Causes, helps identify and understand the underlying sources of errors and the motivations behind human actions that lead to data breaches. Additionally, semi-structured interviews provided further perspectives on the significance of system design and the human role in ensuring EHR security.

Identifying the locations where breaches most frequently occur highlights vulnerabilities to human error-related incidents, which is essential for developing targeted incident response and containment strategies. These findings underscore the pressing cybersecurity challenges within the healthcare sector in protecting patient health information. By examining historical data breaches, this study establishes the groundwork for addressing key research questions and defining the scope of this essay.

2.6 Limitation

One significant challenge in this research study was the lack of a body of literature specifically addressing the human aspect of data breaches and cybersecurity within healthcare in general. First, the literature illustrates that very few studies have focused on the implications of human error in EHR related data breaches. Second, the literature identifies the lack of attention by the international research community to this issue and its impact on EHR adoption and information sharing. Third, the application of STS principles associated with human error in information technology and cybersecurity has not received much attention (Charitoudi et al., 2013). Fourth, the final selection of articles for the systematic literature review included only 40 documents out of an initial 1,071. Section 2.4.2 and Figure 7 provides the process used to down select these documents.

While these limitations highlighted a gap in the literature and presented an opportunity to offer an innovative solution, the absence of relevant studies posed challenges and constrained the foundational knowledge available for this research. The addition of semi-structured interviews with SMEs provided valuable insights, enhancing the depth and confidence of the research and compensating for the scarcity of benchmark data in the field.

Significant effort was also dedicated to grouping the DMUs into homogeneous clusters, as data variability can pose major challenges in establishing accurate performance benchmarks. Since DMUs operate in heterogeneous environments with differing characteristics, a clustering analysis was conducted to create more comparable groups and minimize bias in modeling and hypothesis testing. Several statistical methods were explored across multiple modeling scenarios to determine the optimal number of clusters.

However, despite significant analysis performed across a variety of modeling scenarios, the analysis consistently yielded a single cluster. The analysis incorporated 13 contextual and operational variables, and multiple iterations of principal component analysis (PCA) were performed to reduce dataset dimensionality. PCA results were then used with DBSCAN clustering algorithms to identify the optimal number of clusters. However, the analysis consistently produced a single cluster. To address concerns about heterogeneity, a K-Means algorithm was applied, dividing the DMUs into three high-capacity, mid-capacity, and low-capacity states clusters based on GDP and state population.

2.7 Conclusion, Future Work, and Recommendation

The dissertation concludes that addressing EHR information security threats requires a fundamental shift in the healthcare sector's approach to data security, moving from a focus on purely technical design solutions to a socio-technical dynamic environment. The literature highlights a gap in terms of understanding and modeling of human-computer interactions and the consideration of STS factors when developing solutions. A taxonomy of human error was developed to understand and analyze roots of human error and people’s motivation leading to breaches in information security. To address the gap from the literature, the dissertation presents a socio-technical oriented management framework that applies a STS principles approach to the human-technology interface error challenge in the healthcare sector. The framework is designed to mitigate human error in information security, aiming to enhance the resilience of EHR systems against data breaches and make them less attractive to cybercriminals.

The STS management framework is used to provide an assessment of the relative significance of the locations where data are breached, as a result of human error, and the severity of these breaches to the privacy of patient records. The findings show that network servers and emails are the two most common sites where healthcare data are breached capturing 95% of the 713 million patients' records compromised since 2009. Data breaches in these locations are attributed to vulnerabilities found in multiple STS factors within the healthcare IT systems, such as the lack of reliable identity access management solutions. Thus, future research should focus on investigating these vulnerabilities, generate mitigation options, and investment plans to improve the long term resiliency capability of network servers and emails, aiming at reducing data breach incidents and unauthorized exposure of patient records.

Another valuable direction for future research shall include breaking it up the low-capacity states cluster into two or more sub-groups to create more homogeneous comparison groups. This segmentation can improve the precision and fairness of productivity benchmarking and the regression models by reducing variability within groups, allowing for more meaningful peer comparisons and targeted policy insights for similarly constrained healthcare systems.

Recommendation:

Findings from the literature discussed in this chapter recognize that robust technical design solutions and government policy play an important role in information security, but they are not sufficient to contain data breaches of EHR. An alternative approach is needed, to bridge this gap high-capacity, mid-capacity, and low-capacity DMUs should:

- Adopt the Enhanced Reason's Resiliency Model (Figure 3): The proposed model follows a layered design approach, incorporating STS factors identified in the literature as effective in reducing human error-related data breaches. It represents a cultural shift from the sector's current reliance on purely technical design solutions and toward a socio-technical design environment, where technological, organizational, human, and government factors are integrated to improve EHR information security.

Findings from Chapter 2 also identified the most vulnerable locations within healthcare IT systems where data breaches frequently occur due to human-technology interface errors. To enhance IT systems security, the following proactive measures are recommended for the DMUs. These strategies can strengthen healthcare information security systems, reduce costs, and minimize the number of compromised patient records.

- Predefined Incident Response and Containment Strategies: Develop a comprehensive library of security patches that can be ready available to implement when a data breach incident is identified. This approach helps minimize data exposure time, accelerate patient care service restoration, and reduce overall breach-related costs.
- Routine Penetration Testing and Security Audits: Develop a structured plan to routinely test known system vulnerabilities, such as network servers and emails, and implement security enhancements. Regular assessments and testing will help prevent recurring data breaches and ensure continuous improvement in the IT system security.

Insights from SMEs gathered through semi-structured interviews, along with findings from the literature review, inform these recommendations aimed at strengthening healthcare IT systems. This is achieved by implementing proactive technical measures, strengthening cybersecurity protocols, IAM capabilities, and system monitoring practices, to minimize human-technology interface errors, reduce the risk of data breaches compromising patient records, and ensure continuous improvement in the DMUs IT system security.

2.8 References

[1] Ahola, M., (2020). The Role of Human Error in Successful Cyber Security Breaches. Newspaper-Usecure Blog.

[2] Ajami, R., Al Qirim, N., Ramadan, N., (2012). Privacy Issues in Mobile Social Networks. Scopus Elsevier.

[3] Ajami, S., Arab-Chadegani, R., (2013). Barriers to Implement Electronic Health Records (EHR). Avicena Publisher.

[4] Algarni, A.M., Malaiya, Y.K., (2010). A Consolidated Approach for Estimation of Data Security Breach Costs. University Research-Colorado State University.

[5] Alvarado, W., Triantis, K., (2024). Human Error in Data Breaches of Electronic Health Records (EHR). Journal of Industrial Engineering and Management Studies (JIEMS).

[6] Armitage, A., Keeble-Ramsay, D., (2009). The Rapid Structured Literature Review as a Research Strategy. US-China Education Review.

[7] Bassett, G., Hylender, C.D., Langlois, P., Pinto, A., Widup, S., (2021). Data breach Investigation Report. Verizon Corporation.

[8] Beitollahi, H., Deconinck, G., (2012). A Four-Step Technique for Tackling Distributed Denial of Service Attacks. Scopus Elsevier.

[9] Bowman, S., (2013). Impact of Electronic Health Record Systems on Information Integrity: Quality and Safety Implications. AHIMA.

[10] Bump, J.B., Fan,V.Y., Lanthron, H.E., Yavuz, E.N., (2012). In The Global Fund's Court: Experimentation, Evaluation, and The Affordable Medicine Family. The Lancet.

[11] Callahan, M.E., (2013). Cybersecurity and Hospitals. American Hospital Association.

[12] Carayon, P., (2006). Human Factors of Complex Socio-Technical Systems. Scopus Elsevier.

[13] Charitoudi, K., Blyth, A., (2013). A Socio-Technical Approach to Cyber Risk Management and Impact Assessment. Scientific Research.

[14] Chena, W., LIa, J., Zhang, J., (2011). An Approach to Service Adaptation for Exploratory Application Construction. Scopus Elsevier.

[15] Crema, M., Verbano, C., (2013). Guidelines for Overcoming Hospital Managerial Challenges: A Systematic Literature Review. Dove Press.

[16] Davis, D.R., Kurti, A.N., Skelly, J.M., Redner, R., White, T.J., Higgins, S.T., (2014). A Review of The Literature on Contingency Management in The Treatment of Substance Use Disorders, 2009-2014. Europe PubMed Central (PMC).

[17] Di Nella, A., Mansourian, A., (2021). The Human Error in Cybersecurity. NMS Consulting.

[18] Dolezel, D., McLeod, A., (2019). Managing Security Risk: Modeling the Root Causes of Data Breaches. Health Care Management.

[19] Esmaeilzadeh, P., (2020). How Does IT Identity Affect Individuals' Use Behaviors Associated With Personal Health Devices (PHDs)? An empirical study. Scopus Elsevier.

[20] Evans, M., He, Y., Luo, C., Yevseyeva, I., Janicke, H., Maglaras, L., (2019). Employee Perspective on Information Security Related Human Error in Healthcare: Proactive Use Of IS-CHEC In Questionnaire Form. Research Gate.

[21] Franke, U., Brynielsson, J., (2014). Cyber Situational Awareness: A Systematic Review of the Literature. Scopus Elsevier.

[22] Gabriel, M.H., Noblin, A., Rutherford, A., Walden, A., Cortelyou, K., (2018). Data Breach Locations, Types, and Associated Characteristics Among U.S. Hospitals. The American Journal of Managed Care (AJMC).

[23] Gesulgaa, J.M., Berjameb, A., Moquialac, K.S., Galidod, A., (2018). Barriers to Electronic Health Record System Implementation and Information Systems Resources: A Structured Review. Scopus Elsevier.

[24] Greenacre, M., Groenen, P.J.F., Hastie, T., D'Enza, A.I., Markos, A., Tuzhilina, E., (2023). Principal Component Analysis (PCA). Economic Working Paper Series (1856) – Universitat Pompeu Fabra-Barcelona.

[25] Greenhalgh, G.W., Westhorp, T. G., Buckingham, J., Pawson, R., (2013). RAMESES Publication Standards: Meta-Narrative Reviews. Open Access.

[26] Health Informatics & Health Information Management, (2020). Cybersecurity: How Can It Be Improved in Health Care? University of Illinois, Chicago.

[27] Health Insurance Portability and Accountability Act (HIPAA), (2024). Healthcare Data Breach Statistics. Department of Health and Human Services.

[28] Health Insurance Portability and Accountability Act (HIPAA), (2022). Healthcare Data Breach Statistics. Department of Health and Human Services.

[29] Hofmey, S.A., (1999). An Immunological Model of Distributed Detection and Its Application to Computer Security. University Research- University of the Witwatersrand.

[30] Hung, P.C.K., (2005). Towards a Privacy Access Control Model for e-Healthcare Services. Research Gate.

[31] Information Technology Laboratory- NIST, (2015). Measuring Strength of Identity Proofing. National Institute of Standandards and Technology (NIST).

[32] Isaac, J.T., Zeadally, S., (2011). An Anonymous Secure Payment Protocol in a Payment Gateway Centric Model. Scopus Elsevier.

[33] Jalali, M.S., Kaiser, J.P., (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. Render Internet Publishing.

[34] Kamoun, F., Nicho, M., (2014). Human and Organizational Factors of Healthcare Data Breaches: The Swiss Cheese Model of Data Breach Causation And Prevention. IGI Global.

[35] Katharakisa, G., Katharakib, M., Katostaras, T.,(2013). SFA vs. DEA for Measuring Healthcare Efficiency: A Systematic Review. University Research-International Journal of Statistics and Medical Research.

[36] Keathley-Herring, H., Van Aken, E., Gonzalez-Aleu, F., Deschamps,F., Letens, G., Cardenas-Orlandini, P., (2016). Assessing the Maturity of a Research Area: Bibliometric Review and Proposed Framework.Springer.

[37] Khan, F., Kim, J.H., (2019). Lars Mathiassen, Robin Moore. Data Breach Management: An Integrated Risk Model. Scopus Elsevier.

[38] Khan, N.A., Brohi, S.N., Zaman, N., (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. IEEE Computer Society.

[39] Lahcen, R.A.M., Caulkins, B., Mohapatra, R., Kumar, M., (2020). Review and Insight on the Behavioral Aspects of Cybersecurity. Open Access.

[40] Liginlal, D., Sim, I., Khansa, L., (2008). How Significant is Human Error as a Cause of Privacy Breaches? An Empirical Study and a Framework for Error Management. Scopus Elsevier.

[41] Mackenzie Garrity, (2019). 5% of Hospital IT Budgets Go to Cybersecurity Despite 82% of Hospitals Reporting Breaches. Global Research.

[42] Malatji, M., Von Solms, S., Marnewick, A., (2019). Socio-Technical Systems Cybersecurity Framework. Emerald Publishing Limited.

[43] Meeks, D.W., Smith, M.W., Taylor, L., Sittig, D.F., Scott, J.M., Singh, H., (2014). An Analysis Of Electronic Health Records Related Patient Safety Concerns. Open Access Publishing.

[44] Megas, K., Lam, P., Nadeau, E., (2015). NSTIC Pilots: Catalyzing the Identity Ecosystem. National Institute of Standards Technology (NIST).

[45] Menear, M., Doré, I., Cloutier, A.M., Perrier, L., Roberge, P., Duhoux, A., Houle, J., Fournier, L., (2014). The Influence of Comorbid Chronic Physical Conditions on Depression Recognition in Primary Care: A Systematic Review. Scopus Elsevier.

[46] Miller, R.H., Sim, I., (2004). Physicians' Use of Electronic Medical Records: Barriers and Solutions. Scopus Elsevier. Project Hope.

[47] Milligan, F. J., (2007). Human Factors Theory: Establishing a Culture for Patient Safety- The Role of Education. Scopus Elsevier.

[48] Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G., (2009). Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. Annals of Internal Medicine.

[49] Morgan, S., (2021). The 2020-2021 Healthcare Cybersecurity Report. HERJAVEC Group.

[50] Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E., Bonacina, S., (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Multidisciplinary Digital Publishing Institute (MDPI).

[51] Ouksel, A., Lundquist, D., (2012). A Context-Aware Cross-Layer Broadcast Model for Ad-Hoc Networks. Scopus Elsevier.

[52] Palabindala, V., Pamarthy, A., Jonnalagadda, N.R., (2016). Adoption of Electronic Health Records and Barriers. Journal of Community Hospitals Internal Medicine Perspectives.

[53] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T., (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Scopus Elsevier.

[54] Perneger, T.V., (2005). The Swiss Cheese Model Of Safety Incidents: Are There Holes In The Metaphor? BMC Health Research.

[55] Pfleeger, S.L.,Caputo, D.D., (2012). Leveraging Behavioral Science to Mitigate Cyber Security Risk. The MITRE Corporation.

[56] Ponemon Institute, (2020). Cost of a Data Breach Report. International Business Machines (IBM).

[57] Ponemon Institute, (2022). Cost of a Data Breach Report. International Business Machines (IBM).

[58] Quinn, R.E., (2012). Deep Change Field Guide. Jossey-Bass, John Wiley & Sons, Inc.

[59] Qureshi, Z.H., (2008). A Review of Accident Modelling Approaches for Complex Critical Socio-Technical Systems. Defense Science and Technology Organization.

[60] Raj, M., Fuji, K., Lee, R., Marquard, J., Lee, J., Choi, S.J., (2021). Hospital Productivity After Data Breaches: Difference-in-Differences Analysis. National Institute of Health (NIH).

[61] Razaque, A., Amsaad, F., Khan, M.J., Hariri, S., Chen, S., Siting, C., Ji ,X., (2019). Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain. IEEE Access.

[62] Reason, J., (1990). Human Error: Models and Management. Cambridge University Press.

[63] Rose, S., Borchert, O., Mitchell, S., Connelly, S., (2020). Zero-Trust Architecture. National Institute of Standards Technology (NIST).

[64] Rouached, M., Sallay, H., (2011). An Efficient Formal Framework for Intrusion Detection Systems. Elsevier.

[65] Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A., Herawan, T., (2015). Information Security Conscious Care Behaviour Formation in Organizations. Scopus Elsevier.

[66] Sardi, A., Rizzi, A., Sorano, E., Guerrieri, A., (2020). Cyber Risk in Health Facilities: A Systematic Literature Review. Multidisciplinary Digital Publishing Institute (MDPI).

[67] Sasse, M.A., Brostoff, S., Weirich, D., (2002). Transforming the "Weakest Link": A Human-Computer Interaction Approach for Usable and Effective Security. University College London.

[68] Schoen, C., Davis, K., How, S. K.H., Schoenbaum, S.C., (2006). U.S. Health System Performance: A National Scorecard. Project HOPE–The People-to-People Health Foundation.

[69] Sector Coordinating Councils, (2017). Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients. Department of Health and Human Services.

[70] She, A.H., Zarour, M., Alenezi, M., Sarkar, A.K., Agrawal, A., Kumar, R., Khan, R.A., (2020). Healthcare Data Breaches: Insights and Implications. Multidisciplinary Digital Publishing Institute (MDPI).

[71] Smet, M., (1982). Cost Characteristics of Hospitals. Social Science & Medicine. Europe PubMed Central (PMC).

[72] Snyder, H., (2019). Literature Review as A Research Methodology: An Overview and Guidelines. Scopus Elsevier.

[73] The White House, (2021). Improving the Nation's Cybersecurity. Executive Order 14028.

[74] Torraco, R.J., (2005). Writing Integrative Literature Reviews: Guidelines and Examples. SAGE Journals.

[75] Torres-Tomas, J., Spolaˆora, N., Alvares-Chermana, E., Mona, M.C., (2014). A Framework to Generate Synthetic Multi-Label Datasets. Scopus Elsevier.

[76] Tran, P., (2021). Are Cybersecurity Issues Delaying Healthcare AI Adoption? Ferrum, Domain Knowledge.

[77] Transfield, D., Denyer, D., Smart, P., (2003). Towards a Methodology for Developing-Evidence Informed Management Knowledge by Means of Systematic Review. University Research-British Journal of Management.

[78] Trist, E., Bamforth, K., (1951). Some Social and Psychological Consequences of the Longwall Method of Coal Getting. Human Relations.

[79] Vargheese, R., Prabhudesai, P., (2014). Securing B2B Pervasive Information Sharing Between Healthcare Providers: Enabling the Foundation for Evidence Based Medicine. Scopus Elsevier.

[80] Warketin, M., Willison, R., (2017). Behavioral and Policy Issues in Information Systems Security: The Insider Threat. European Journal of Information Systems.

[81] Warketin, M., Willison, R., (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. Journal Storage (JSTOR).

[82] Whitworth, B., (2009). The Social Requirements of Technical Systems. University Research- IGI Global.

[83] Williams, P.A.H., Woodward, A.J., (2020). Cybersecurity Vulnerabilities in Medical Devices: A Complex Environment and Multifaceted Problem. Publication Medication Central (PMC).

[84] Workgroup for Electronic Data Interchange, (2017). The Rampant Growth of Cybercrime in Healthcare. FORTINET.

[85] Yadav, J., Sharma, M., (2013). A Review of K-Mean Algorithm. International Journal of Engineering Trends and Technology (IJETT), Volume 4, Issue 7.

[86] Yan, Z., Robertson, T., Yan, R., Park, S.Y., Bordoff, S., Chen, Q., Sprissler, E., (2018). Finding the Weakest Links in the Weakest Link: How Well Do Undergraduate Students Make Cybersecurity Judgment? Scopus Elsevier.

[87] Yasnoff, W.A. (2016). A Secure and Efficiently Searchable Health Information Architecture. Scopus Elsevier. Scopus Elsevier.

[88] Zimmermann, V., Renaud, K., (2019). Moving from a ‘Human-as-Problem” to a ‘Human-as-Solution” Cybersecurity Mindset. Scopus Elsevier.

Chapter 3.0 - Essay 2: Unintended Consequences from Adoption of EHR Technology: Impact of Human Error Data Breaches on the Productivity Performance of States Healthcare Systems

Abstract

The productivity performance of the U.S. healthcare system remains a primary concern to government and industry leaders (Schoen et al., 2006). Some literature concludes that EHR technology is an important tool that improves healthcare quality of services and lowers the cost of the healthcare sector (Yasnoff, 2016). But, there are mixed results found in the literature about the healthcare providers' perceptions of the benefits of EHR to patient care performance (Atasoy et al., 2019).

This chapter examines the productivity performance of DMUs (States) over time using Malmquist productivity index (MPI), a valuable tool for analyzing and comparing productivity changes and efficiency improvements. The MPI measures how DMUs implement data security safeguards to enhance productivity within EHR technology, driving technological advancements to improve patient care while protecting sensitive information. The essay applies MPI to three state clusters, high-capacity, middle-income, and low-capacity states that have adopted EHR technology, aiming to assess the unintended consequences, particularly information privacy concerns stemming from human error in healthcare data breaches.

Despite privacy concerns resulting from human error data breaches, the productivity performance of states healthcare systems (DMUs) has increased since 2009. The pursuit of improving the productivity of DMUs has led to the development of various models designed to enhance performance. One focus has been on reducing privacy concerns related to the protection of personal health information, minimizing errors in health information management, and improving IT systems that store patients' health records. Reducing privacy concerns enhances patient trust, leading to more accurate data sharing, improved diagnoses, and streamlined patient care delivery. Further, strengthening data protection reduces operational disruptions from data breaches, lowering administrative costs and ensuring consistent healthcare services. Improved

security also facilitates greater adoption of digital health technologies, optimizing services and boosting overall productivity in the healthcare sector.

State healthcare systems are effective DMUs for MPI analysis due to their structured inputs (number of managed patients, healthcare expenditures, etc.) and measurable outputs (lengths of hospital stay, deaths). These metrics enable assessing how input resources are utilized to drive productivity and performance changes over time. Although these DMUs may exhibit heterogeneity, they still are comparable because they operate under the same federal regulatory framework. This standardization allows for meaningful benchmarking while still accounting for variations in operational productivity across different states.

The MPI results revealed an overall increase in productivity performance for DMUs. Despite a decline in productivity performance among high-capacity and mid-capacity states over time, improvements in low-capacity states have helped offset the overall downturn. These findings suggest that larger population of patients in high-capacity and mid-capacity states make their healthcare systems more vulnerable to cyberattacks. Investments in their IT security systems seem insufficient, as they continue to face vulnerabilities that cyber attackers continue to exploit. In contrast, low-capacity states appear to have effectively balanced EHR technology advancements with measures to address information privacy concerns, ultimately leading to improved patient care services over time.

KEYWORDS: Data Envelopment Analysis, Economic Production, Productivity Performance, Electronic Health Records, Information Privacy, Malmquist Productivity Index, States Healthcare Systems.

3.1 Introduction

"Information technology has been one of the leading drivers of globalization, and it may also become one of its major victims." Evgeny Morozov

The purpose of this essay is to assess the unintended consequences of EHR technology adoption, particularly information privacy concerns stemming from human error in healthcare data breaches and their impact on patient care services. Protecting patient health information is essential for enhancing the quality of patient care services, as it cultivates patient trust in the system and has the potential to reduce the future burden of financial penalties and legal consequences for healthcare organizations.

The Industrial Revolution has been seen by many as the most profound display of innovation in human history, because of its major impact on people's daily lives. Perhaps what marked in history the impact of the Industrial Revolution was the merger of human and technology interactions. Technology adoption and key inventions shaped every existing sector of human activity along industrial lines, while also creating many new enhancements in industrial processes (Wilkinson, 2022).

The abundance of data available in the healthcare sector presents significant opportunities, such as new methods for data collection, and the potential for greater information insights. Advances in communications and the spread of IT have generated an ability to create and share exponentially growing amounts of information more quickly and widely than ever before. However, these technological advances have also brought unintended consequences particularly to information privacy concerns, which are impacting the quality of patient care services provided by DMUs.

Healthcare investments in automated computing technologies are enabling the sector to provide better services to patients. In 2004, the Bush Administration established the Office of the National Coordinator for Health Information Technology (ONC) to help bring the healthcare sector into the digital age (DHHS Federal Register, 2009). Then, in 2009, Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act to spur greater action on digitizing health and moving away from

the waste and errors associated with a paper-based health system (Esmaelilzadeh, 2020). HITECH encourages healthcare providers to adopt EHR and improve privacy and security protections (Matthews, 2018).

As established in previous chapters, EHR have the potential to significantly enhance the productivity performance of DMUs (HIPAA, 2021). In the application of MPI in this essay, the productivity performance of the DMUs is defined as their ability to provide enhanced healthcare services (output) while utilizing input resources such as EHR technology and funds generated from healthcare services effectively. Productivity performance is measured by evaluating how well these resources are converted into desired outcomes, such as reduction in deaths, shorter lengths of stay at healthcare facilities, and longer life span.

EHR have improved patient care satisfaction and disease diagnoses by making patient health information accessible to healthcare providers, thus enabling better healthcare outcomes. However, the protection and security of patient health information against data breaches are considered one of the most significant challenges obstructing the adoption of EHR and the sharing of information in the healthcare industry (Tran, 2021). Specifically, healthcare data are more sensitive than other types of data because any manipulation can lead to faulty treatment, with potentially fatal and irreversible consequences for patients (She et al., 2020).

The findings from this essay offer insights into the productivity performance of the DMUs over time, particularly in their implementation of data security safeguards aimed at enhancing patient care services while protecting patient information from breaches. EHR are seen by the government and many experts in the field as the systems that provide the patient care services (transformation processes). It constitutes a key component of the healthcare sector that needs to improve its productivity and lower the cost of healthcare services to patients (HIPAA, 2021). The practical contribution from this essay to the Economic Production Theory literature lies in its identification of traits and models from DMUs that have effectively balance the implementation of EHR

technological advancements with the need to address information privacy concerns, ultimately leading to improved patient care services. Additionally, the MPI results provide an indication of how well DMUs comply with government privacy regulations, such as HIPAA, demonstrating their commitment to reducing the risks of privacy breaches.

3.2 Technical Background

Today's organizations face difficult decisions between accepting cybersecurity risks in exchange of creating an operating environment that increases productivity. For example, despite cybersecurity concerns, organizations allow their personnel to work remotely because it improves the employee satisfaction which leads to productivity increases. Similarly, the cost of a data breach can create significant financial burden to the organization, but losses due to low productivity can prevent organizations from meeting their financial goals. These situations present a management decision dilemma about unintended consequences from technology adoption.

The interaction between humans and technology has an impact on economic efficiency (Zhao, 2018). Understanding and mitigating the impact of human-technology interface errors are essential components of effective economic production management (Emami-Mehrgani et al., 2016). Concepts from the economic production theory are used to measure productivity performance of DMUs employing input and output benchmarking performance analysis. The benchmarking analysis examines how productivity and technological advancements have evolved over time in high-capacity, mid-capacity, and low-capacity states that have adopted EHR technology.

The Economic Production Theory explained by Equation (1), provides the foundation to understand the process of converting inputs (e.g., labor, capital, and materials) into outputs (goods and services). It can be seen as a framework to analyze production efficiency, optimize resource allocation, and understand the relationships between inputs and outputs.

$$\textit{Productivity} = \frac{\textit{Output}}{\textit{Inputs}} \qquad \text{Equation (1)}$$

Represented by the function: $Q_{max} = f(L, K, M)$;

where Q is the output; and L, K, M are inputs such as labor, capital and materials.

The MPI calculates the relative performance of a DMU at different periods of time using the technology of a base period. The MPI is based on the data envelopment analysis (DEA) modeling (Färe et al., 1994). DEA, a modeling approach that seeks to identify the productivity frontier using linear programming models, evaluates the relative efficiency between DMUs using input and output variables. The MPI as an application from DEA introduces a dynamic application of the Economic Production Theory, enabling organizations and policymakers to track and understand changes in productivity between DMUs over time. The index is calculated as the product of two productivity components: efficiency change (EC) and technological change (TC).

$$MPI = EC*TC$$

$$M^o(x_t, y_t, x_{t+1}, y_{t+1}) = \left[\frac{D^o_{t+1}(x_{t+1}, y_{t+1})}{D^o_{t+1}(x_t, y_t)}\right] * \left[\frac{D^o_t(x_{t+1}, y_{t+1})}{D^o_{t+1}(x_{t+1}, y_{t+1})} * \frac{D^o_t(x_t, y_t)}{D^o_{t+1}(x_t, y_t)}\right]^{1/2} \qquad \text{Equation (2)}$$

Efficiency Change (EC) Technological Change (TC)

$$M^o(x_t, y_t, x_{t+1}, y_{t+1}) = \left[\frac{D^o_t(x_{t+1}, y_{t+1})}{D^o_t(x_t, y_t)} * \frac{D^o_{t+1}(x_{t+1}, y_{t+1})}{D^o_{t+1}(x_t, y_t)}\right]^{1/2} \qquad \text{Equation (3)}$$

D^0_t: *Efficiency of DMU's performance at time t related to the baseline frontier at time 0.*
D^0_{t+1}: *Efficiency of DMU's performance at time t+1 related to the baseline frontier at time 0.*

x_t: input variable at time t; x_{t+1}: input variable at t+1
y_t: output variable at time t; y_{t+1}: output variable at t+1

(Huerta et al., 2012)

EC, calculated using the math model from Equation (2), measures whether the DMU has improved its use of resources relative to best practice economic frontier. If EC is greater than 1, it means the DMU is becoming more efficient, possibly by improving management or reducing waste. An EC of less than 1 indicates a decline in productivity, or the DMU is falling behind the frontier.

TC, calculated using the math model from Equation (2), assesses shift in the production frontier due to technological improvements or regressions. A TC greater than 1 suggests that new technologies or processes have been implemented, pushing the production frontier outward. Conversely, a TC of less than 1 indicates technological regression or falling behind in innovation.

The MPI is calculated as the product of two productivity components: EC and TC, Equation (3). When the MPI is greater than one, it suggests that the DMU has improved in productivity over time, meaning it has effectively utilized resources, advanced technological capabilities, or optimized processes to improve patient care services. When the MPI is equal to 1.0, the DMU's productivity remains unchanged, indicating that there has been no significant change in efficiency or technological advancements during the performance period. But, when the MPI is less than one, the DMU has experienced a decline in productivity, meaning there may be resource misallocation, technologic deterioration, or increased inefficiencies negatively impacting patient care services.

3.3 Research Problem

Mixed results are found in the literature about the healthcare providers' perceptions of the benefits of EHR to patient care performance (Atasoy et al., 2019). Some literature concludes that EHR technology is an important tool that improves healthcare quality of services and lowers the cost of the healthcare sector (Yasnoff, 2016). The HIPAA Journal (HIPAA, 2021) reports that since the 2004 healthcare digitization initiative, EHR have been the leading healthcare technology enabling the sector to increase information sharing between stakeholders; thus, reducing the number of patient medical tests and the time it takes to perform diagnosis. Consequently, lowering costs and improving patient care quality and the overall productivity performance of healthcare providers.

Despite the significant benefits of EHR adoption in improving patient care, unintended consequences have emerged, particularly human-error data breaches compromising patient information privacy. Poor EHR system designs and improper usage have

contributed to errors that have exposed millions of patient records, raising serious concerns about patient safety, information security, and healthcare service quality (Appari et al., 2013). Additionally, these breaches have negatively impacted the productivity performance of healthcare providers, leading to legal disputes, operational disruptions, loss of patient trust, and substantial financial costs (Bowman, 2013). Healthcare remains a primary target for attackers due to its reliance on outdated IT security systems, which create significant vulnerabilities and continually compromise patient information privacy (Ponemon Institute, 2024). Given the growing reliance on EHR systems, it is critical to investigate how human-technology interface vulnerabilities contribute to these breaches and explore strategies to mitigate their impact on healthcare productivity and patient care.

Patient care service satisfaction has been positively linked with access to healthcare records (Blaya et al., 2007). The adoption of EHR aims to improve patient satisfaction by providing better access to patient clinical information, reducing the time healthcare providers spend searching information, and allowing them to focus more time on patient care and communication (Kazley et al., 2012). Under HIPAA regulations, patients have the legal right to access their EHR, and healthcare providers continue to adopt EHR not only to improve patient interaction but also to comply with HIPAA regulations (Kisekka, et al., 2018).

Essay 2 examines patients' information privacy concerns, as unintended consequences of EHR technology adoption and their impact to patient care services. Data breaches caused by human-technology interface error serve as measure of patient's information privacy concerns. The primary objective of this essay is to test a hypothesis that clarifies the mixed findings in the literature regarding the benefits of EHR technology adoption on patient care service performance. To achieve this objective, the essay uses empirical evidence from DHHS datasets on EHR adoption and healthcare data breaches.

The hypothesis states that, ***despite increasing patient privacy concerns due to healthcare data breaches, the adoption of EHR technology has contributed to productivity improvements in DMUs through technological advancements and efficiency gains.*** To test this hypothesis, MPI is calculated to assess productivity changes over time in the performance of DMUs in delivering patient care. The MPI model incorporates input variables such as healthcare providers adopting EHR technology, healthcare data breaches, managed patients, and healthcare expenditures per capita, with EHR technology as the transformation process. The Output variables include: total deaths, length of stay, and life expectancy. Figure 15 illustrates the input-output relationship with EHR technology as the transformation process, while Table 21 provides a detailed description of these variables.

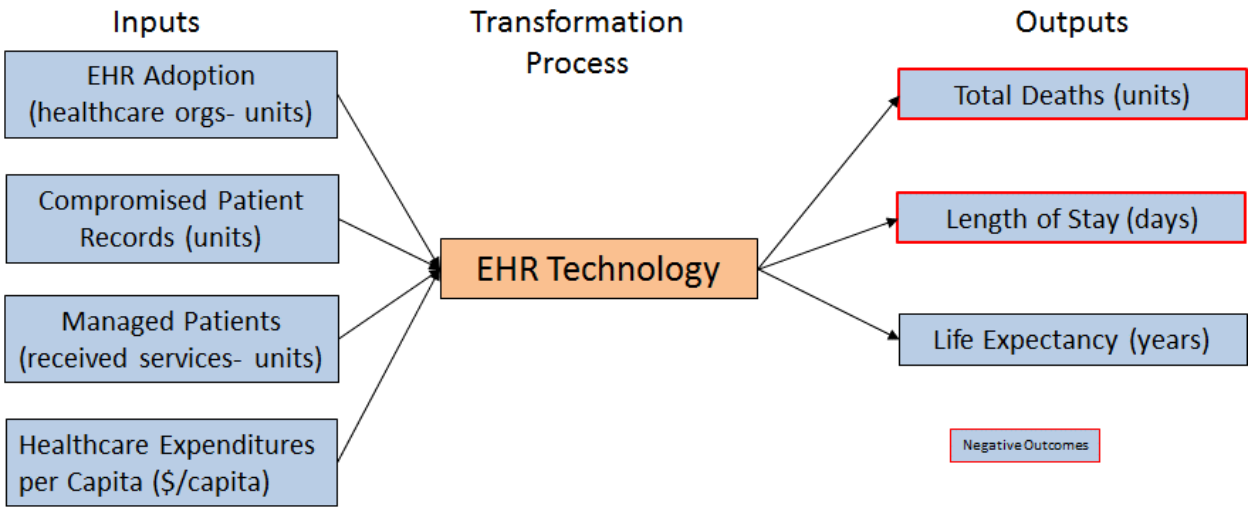


Figure 15: Input / Output Variables and EHR Transformation Process for MPI Assessment

This essay seeks to answer the following question: ***how have information privacy concerns arising from adoption of EHR technology impact patient care services over time among healthcare providers in different states?*** Understanding this relationship will enable healthcare management make more informed resource allocation decisions, effectively balancing EHR technology implementation with safeguard measures to address patient information privacy concerns in the midst of the escalating number of data breaches in the healthcare sector.

3.4 Research Method

3.4.1 Data

Semi-Structured Interviews

Table 16 includes the questions asked to the SMEs to inform the semi-structured interviews and qualitative data requirements for Essay 2.

Essay 2: Unintended Consequences from Adoption of EHR Technology		
Do Security Breaches Affect Organizations' Performance?	How Do Healthcare Professionals Navigate Privacy Concerns?	What are People's Perceptions of Organizations After Privacy Violation Incidents?

Table 16: Essay 2 SMEs Interview Questions

Quantitative Data Collection

Comprehensive quantitative datasets support the modeling and hypothesis testing and the findings presented in this chapter. The datasets described in Chapter 1 and 2 are also used to support modeling and hypotheses testing of the foundational data for Chapters 3 and 4 of this research. These datasets include all reported cybersecurity incidents from DMUs submitted to the DHHS OCR, as mandated by the HIPAA Privacy and Security Rules since 2009. They contain data breach incidents reported by healthcare organizations across all 50 states and the District of Columbia (HIPPA, 2024).

The data used for this essay also include healthcare performance metrics: demographic information, and economic data. These data come from government entities, including DHHS, U.S. Census Bureau, the National Center for Health Statistics, the American Hospital Association, and state health departments. With hundreds of recorded events for multiple input and output variables, the datasets support benchmarking and statistical modeling providing the confidence level for testing the hypothesis in this essay. Table 17 illustrates the list of all datasets and their sources used in Essay 2.

Data by State	Category	Range	Source
Healthcare Expenditure per Capita	Healthcare Economics and Demographics	1991-2022	DHHS- Centers for Medicare & Medicaid Services, Office of the Actuary, National Health Statistics Group
Length of Stay	Healthcare Services	1999-2022	American Hospital Association (AHA) Annual Survey
Managed Patients	Healthcare Services	1999-2022	American Hospital Association (AHA) Annual Survey
Life Expectancy	Health Status	1959-2020	National Center for Health Statistics
Deaths	Health Status	2000-2022	DHHS -Centers for Disease Control and Prevention's National Center for Health Statistics
Hospital Adoption of EHRs	Business Process Modernization	2009-2020	DHHS -Centers for Disease Control and Prevention's National Center for Health Statistics
Healthcare Nursing Facilities Adoption of EHRs	Business Process Modernization	2009-2019	DHHS -Centers for Disease Control and Prevention's National Center for Health Statistics
Data Breach Incidents	Information Security	2009-2024	DHHS- Office of Civil Rights

Table 17: Quantitative Datasets with Sources and Data Range Used in Essay 2

To facilitate this assessment, a Microsoft Excel database was created to collect all input and output variables used for the MPI calculation. The database spans events from 2009 to 2022 across all 50 states and the District of Columbia. Table 18 outlines a sample of the database with all the input / output variable fields used for the MPI calculation.

DMU	Year	Healthcare - Hospitals Acute Care (Input)	Healthcare Nursing Facilities Non-Acute Care (Inpu	Healthcare Data Breaches (Input	Number of Managed Patients (hospital admissions and outpatient visits) Input	Healthcare Expenditures per Capita BY22$ (Input)	Total Deaths (Output)	Length of Stay (Output)	Life Expectancy (Output)
Alabama	2009	10.80	41.56	0	9,960,267	8,624	47,470	5.50	75.3
Alaska	2009	5.06	3.42	0	1,825,465	11,663	3,618	5.10	77.8
Arizona	2009	14.40	27.58	0	7,509,914	8,017	45,816	5.95	75.8
Arkansas	2009	11.18	43.56	0	5,442,241	8,489	28,673	4.51	79.1
California	2009	72.03	211.92	0	51,704,694	8,467	232,736	5.21	80.3
Colorado	2009	25.11	44.97	0	9,206,616	7,994	31,173	5.23	79.7
Connecticut	2009	11.20	28.40	0	8,690,382	11,897	28,585	5.09	80.5
Delaware	2009	1.61	7.92	0	1,860,514	11,438	7,534	5.37	78.2
District of Columbia	2009	3.20	2.69	1	2,454,883	14,597	4,834	6.28	73.0

Table 18: Dataset of Input / Output Variables Used for MPI Calculations (2009-2022)

Two outputs variables, total deaths and length of stay, are considered undesirable variables to calculate the productivity indices, because increases in input variables should not increase the value for these variables. Addressing undesirable outputs is important when assessing productivity in systems where certain outputs are unfavorable. To account for this in MPI measurement, the values for the total deaths and length of stay were transformed using the large number approach (Dyson et al., 2001). This approach is a regularly used technique in benchmarking analysis for managing undesirable outcomes. The method ensures non-negativity by scaling

negative output variables for inclusion in the MPI model. Table 19 presents a sample of the database with the undesirable variables transformed into positive outcomes.

DMU	Year	Healthcare - Hospitals Acute Care (Input	Healthcare Nursing Facilities Non-Acute Care (Inpu	Healthcare Data Breaches (Input)	Number of Managed Patients (hospital admissions and outpatient visits) Input	Healthcare Expenditures per Capita BY22$ (Inpu	Transformed - Reduced Deaths (Output)	Transformed-Reduced Length of Stay (Output)	Life Expectancy (Output)
Alabama	2009	10.80	41.56	0	9,960,267	8,623.990	369,091.250	7.255	75.3
Alaska	2009	5.06	3.42	0	1,825,465	11,663.257	412,943.250	7.660	77.8
Arizona	2009	14.40	27.58	0	7,509,914	8,016.955	370,745.250	6.804	75.8
Arkansas	2009	11.18	43.56	0	5,442,241	8,488.942	387,888.250	8.253	79.1
California	2009	72.03	211.92	0	51,704,694	8,467.116	183,825.250	7.552	80.3
Colorado	2009	25.11	44.97	0	9,206,616	7,993.765	385,388.250	7.526	79.7
Connecticut	2009	11.20	28.40	0	8,690,382	11,896.523	387,976.250	7.668	80.5
Delaware	2009	1.61	7.92	0	1,860,514	11,438.177	409,027.250	7.393	78.2
District of Columbia	2009	3.20	2.69	1	2,454,883	14,597.487	411,727.250	6.481	73.0

Table 19: Dataset of Input / Output Variables by DMU with Negative Outcomes Variables Transformed Using Dyson's Large Number Approach (2009-2022)

Following this transformation, all input/output variables were normalized using “Max-Min” linear normalization approach to avoid bias due to difference in scale or measurement units in the MPI algorithm calculations. Table 20 presents a sample of the database with input / output normalized variables.

DMU	Year	Xn = X-Xmin/(Xmax-Xmin) Healthcare - Hospitals Acute Care (Input)	Xn = X-Xmin/(Xmax-Xmin) Healthcare Nursing Facilities Non-Acute Care (Input)	Xn = X-Xmin/(Xmax-Xmin) Healthcare Data Breaches (Input)	Xn = X-Xmin/(Xmax-Xmin) Number of Managed Patients (hospital admissions and outpatient visits) Input	Xn = X-Xmin/(Xmax-Xmin) Healthcare Expenditures per Capita BY22$ (Input)	Xn = X-Xmin/(Xmax-Xmin) Transformed -Total Deaths (Output)	Xn = X-Xmin/(Xmax-Xmin) Transformed-Length of Stay (Output)	Xn = X-Xmin/(Xmax-Xmin) Life Expectancy (Output)
Alabama	2009	0.0219169	0.0412523	0.0000015	0.1364824	0.1229585	0.8669668	0.8004525	0.4576271
Alaska	2009	0.0102685	0.0033922	0.0000015	0.0105451	0.3358356	1.0000000	0.8573056	0.6694915
Arizona	2009	0.0292225	0.0273715	0.0000015	0.0985478	0.0804404	0.8719845	0.7371631	0.5000000
Arkansas	2009	0.0226880	0.0432330	0.0000015	0.0665375	0.1134994	0.9239910	0.9405205	0.7796610
California	2009	0.1461735	0.2103319	0.0000015	0.7827408	0.1119706	0.3049279	0.8422585	0.8813559
Colorado	2009	0.0509568	0.0446367	0.0000015	0.1248149	0.0788161	0.9164068	0.8385723	0.8305085
Connecticut	2009	0.0227286	0.0281903	0.0000015	0.1168230	0.3521740	0.9242580	0.8585324	0.8983051
Delaware	2009	0.0032672	0.0078605	0.0000015	0.0110877	0.3200704	0.9881201	0.8199458	0.7033898
District of Columbia	2009	0.0064939	0.0026670	0.0151515	0.0202893	0.5413556	0.9963110	0.6918936	0.2627119

Table 20: Dataset of Input / Output Variables by States Normalized Using Max/Min Approach (2009-2022)

3.4.2 Approach

Findings from the literature and semi-structured interviews guided the selection of input and output variables for the benchmarking analysis used in this chapter. Table 21 provides a detailed overview of the input and output variables, including their descriptions and justification for selection.

Input Variable	Description	Justification
EHR Adoption (Units)	Two Input Variables are Used to Measure EHR Adoption: Hospitals Acute Care and Healthcare Nursing Facilities Non-Acute Care. They are Considered the Two Biggest Healthcare Providers. Government Healthcare Providers were not Included in These Variables.	Represents an Efficient Way of Keeping Patient Records for Fastest Diagnosis and Reduction in Service Duplication
Data Breach Incidents (Units)	Number of Data Breaches Where 500 or More Records were Compromised as a Result of a Human-Technology Interface Error.	Capture the Risk Incurred from Digital Technology Used to Improve Healthcare Processes
Managed Patients (Units)	Number of Patients Who Received Services or were Under Care, Treatment, of Supervision in a Healthcare Facility in a Year.	Reflect Infrastructure and Processes for Delivering Healthcare Services
Healthcare Expenditures ($/Capita)	Average Annual $s Spent on Healthcare Services by Each Resident of a State.	Represent Payments for Services that are Necessary for Healthcare Delivery
Output Variable	**Description**	**Justification**
Total Deaths* (Units)	A Variable that Accounts for the Total Number of Deaths Reported by Each State in a Given Year.	Reflect the Efficiency of Healthcare Services Leading to Save Lives
Length of Stay* (Days)	A Variable that Measures the Length of Time Between a Patient's Admittance to and Discharge from a Healthcare Provider.	Captures the Quality and Effectiveness of Services to Reduce the Amount of Time a Patient Spent in a Healthcare Facility
Life Expectancy (Years)	A Variable that Measures the Average Number of Years a Person from a State is Expected to Live.	Represents the Primary Outcome of Healthcare Service Efforts.

*Undesirable Outcomes

Table 21: Input / Output Variables Used for Calculating the MPI

The datasets were organized by year and states, and plotted to conduct a comparison of adoption trends and data breach incidents over time. States were grouped by high-capacity, mid-capacity, and low-capacity state clusters. The MPI benchmarking analysis examined productivity changes from 2009 to 2022, utilizing over 4,000 observations across four input and three output variables. MPI was applied to evaluate the relative productivity of different DMUs over time, using the technology of a base period (Wang et al., 2011). The base period selected was 2009, the year that the HITECH policy was enacted to drive the adoption and meaningful use of health information technology. Table 22 provides descriptive statistics of all the input and output variables used for the MPI calculations.

Input / Output Variables	EHR Adoption Hospitals (I)	EHR Adoption Clinics (I)	Human Error Data Breaches (I)	Managed Patients (I)	Healthcare Expenditures (I)	Total Deaths (O)	Length of Stay (O)	Life Expectancy (O)
Meta (All States)								
Average	73	188	6	14,775,982	11,000	55,014	6	78
Std Deviation	71	190	9	14,239,908	2,229	55,893	1	2
Max	493	1,008	66	65,738,336	21,146	333,249	10	82
Min	1	0	0	1,144,319	6,869	3,618	4	71
Observations	714	714	714	714	714	714	714	714
Rich States								
Average	236	578	22	53,931,710	11,037	208,237	6	80
Std Deviation	143	288	19	7,068,879	2,702	52,836	1	1
Max	493	1,008	66	65,738,336	18,820	333,249	7	81
Min	34	85	0	38,685,291	8,143	146,432	4	75
Observations	42	42	42	42	42	42	42	42
Mid-Income States								
Average	106	314	10	27,049,477	10,905	99,822	5	79
Std Deviation	55	186	9	10,217,719	1,947	42,016	1	1
Max	215	786	41	48,626,347	18,116	261,369	9	81
Min	18	45	0	12,103,845	7,411	48,146	4	74
Observations	154	154	154	154	154	154	154	154
Poor States								
Average	50	118	3	7,952,317	11,025	29,269	6	78
Std Deviation	39	105	4	5,358,609	2,268	19,880	1	2
Max	153	477	26	27,383,386	21,146	91,130	10	82
Min	1	0	0	1,144,319	6,869	3,618	4	71
Observations	518	518	518	518	518	518	518	518

Table 22: Descriptive Statistics of Input / Output Variables for State Clusters (009-2022)

A hybrid approach was employed to test the dissertation hypothesis of this essay. To assess the statistical significance in mean values across the DMUs cluster groups, MPI results were analyzed using a one-way analysis of variance (ANOVA). Additionally, regression analysis was performed to explore the relationship between the MPI results from each state cluster and two factors from the STS management framework presented in Figure 12 from Chapter 2. These factors include “Human in the Loop,” represented by compromised patient records due to human error data breaches, and “Government Regulation,” represented by HIPAA monetary penalties. These contextual variables were used to conduct the ANOVA Test used for testing the hypothesis in this essay:

> ***H2:*** **Despite increasing patient privacy concerns due to healthcare data breaches, the adoption of EHR technology has contributed to productivity improvements in DMUs through technological advancements and efficiency gains.**

3.5 Results and Discussion

Qualitative - Semi-Structured Interview Results

Semi-structured interviews provided valuable insights from cybersecurity and healthcare professionals on nuances in patient care practices that were not evident in the literature. Insights from these real world experts in cybersecurity and healthcare informed the variables selection for the MPI assessment conducted in this Essay 2, which evaluates the productivity performance of the DMUs. The interviews also highlighted new areas for future research to enhance understanding of healthcare information privacy concerns. More importantly, the insights gained were used to validate findings from the literature, ensuring that the selection of input and output variables, as well as the application of statistical and benchmarking methods effectively supported the dissertation hypotheses.

Table 23 summarizes findings from the semi-structured interviews, including takeaways, qualitative results, and how the findings inform this dissertation. Additional details are also included in Appendices F thru J at the end of the dissertation.

Literature Gap	Interviews Takeaway	Interview Findings	Qualitative Results	How Findings Inform the Research
Essay 2: Determine impact of unintended consequences from EHR adoption to performance of state health organizations	Security breaches affect performance of healthcare organizations	Security breaches affect performance • Cause degradation in patient care services • Increase cost of operations for organizations • Contribute to loss of competitive advantage • Cause erosion of trust with business partners and patients Mitigation strategies to prevent data breaches • Promote system protective measures • Limit system access (need to know) • Improve data transmission Perceptions after privacy violation • Mixed results about trust in organization processes • Create concerns about data sharing	• Identify differences in organizations' system capability to protect data, and impacts to cost and patient care services • Insight into variable selection for clustering and performance index • Highlight impact of digitization to performance improvement	Clustering Variables • Gross domestic product (GDP) • State population MPI Variables • EHR Adoption • Data Breach Incidents • Managed Patients • Healthcare Expenditures/Capita • Total Deaths • Length of Stay • Life Expectancy

Table 23: Essay 2 Results from Semi-Structured Interviews and How the Findings Inform the Research Study

Quantitative Data Results

Figure 16 presents data breaches and EHR technology adoption from healthcare providers from within all 50 states and the District of Columbia. Most healthcare providers, hospitals and healthcare nursing facilities have adopted EHR technology making the transition from paper to digital records despite increases in data breaches and data privacy concerns. However, since 2015 the adoption has remained relatively flat.

The datasets show differences in the adoption levels of the different DMUs. The DHHS OCR continues to report an increase in healthcare breaches despite efforts by government policy makers to mandate a focus in the protection of patient healthcare data. The loss of patient health information presents identity theft and fraud risks to patients and health plan holders. More importantly, it places risk to patient health if the records are compromised and become a target to induced treatment error.

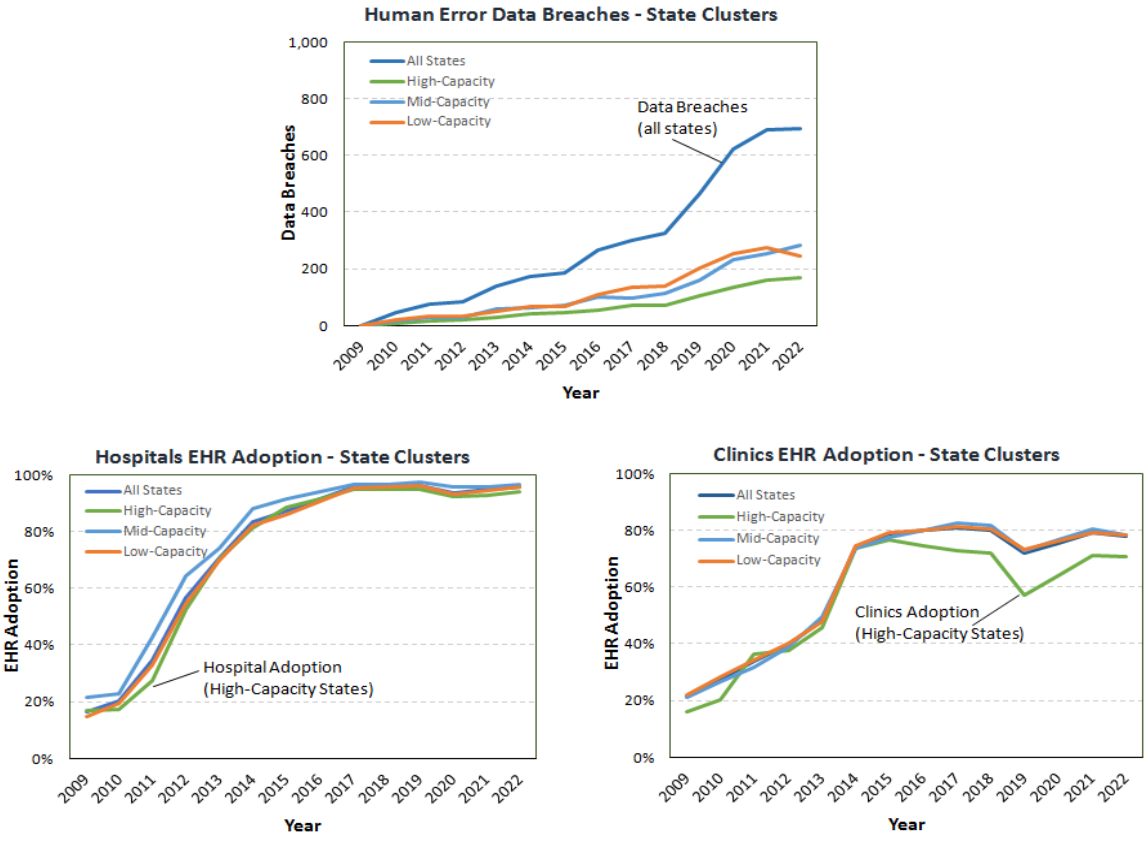


Figure 16: Rising Trend of Data Breaches and EHR Technology Adoption Over the Years (DHHS ONC Health IT, 2022)

MPI Assessment

The Malmquist Performance Index (MPI) was used for analyzing and comparing the productivity changes and efficiency improvements of the DMUs. The MPI results from Table 24 indicate an overall improvement in productivity performance among the DMUs across all states from 2009 to 2022 (Mean = 1.095). However, a contrasting trend is observed when examining the state clusters. While high-capacity states (Mean = 0.798) and mid-capacity states (Mean= 0.873) experienced a decline in productivity over time, low-capacity states (Mean = 1.167) showed significant improvement, effectively offsetting the declines observed in the other clusters. Additional details are included in Appendix B.

Variable	State Cluster	Observations	Mean	STD Deviation	Max	Min
EC	Meta	714	1.032	0.076	1.451	0.981
	High-Capacity	42	1.000	0.000	1.000	1.000
	Mid-Capacity	154	1.009	0.011	1.033	1.000
	Low-Capacity	518	1.019	0.051	1.221	0.981
TC	Meta	714	1.082	1.180	9.325	0.829
	High-Capacity	42	0.798	0.017	0.808	0.779
	Mid-Capacity	154	0.869	0.036	0.925	0.793
	Low-Capacity	518	1.158	1.382	9.325	0.848
MPI	Meta	714	1.095	1.179	9.325	0.820
	High-Capacity	42	0.798	0.017	0.808	0.779
	Mid-Capacity	154	0.873	0.036	0.923	0.797
	Low-Capacity	518	1.167	1.381	9.325	0.859

Table 24: Summary of MPI Results by State Clusters (2009-2022)

The TC index signals inefficiencies in applying or maintaining adopted technology, with high-capacity states (TC = 0.798) and mid-capacity states (TC = 0.869) showing signs of technological regression. To further investigate these findings, a sensitivity MPI analysis was conducted. The findings show that removing the “Data Breach Incidents” input variable led to an increase in the TC index for high-capacity and mid-capacity states, while the TC index for low-capacity states declined. This suggests that data breaches play a critical role in shaping the productivity scores of the DMUs. The MPI results indicate that low-capacity states perform better in safeguarding patient data privacy compared to high-capacity and mid-capacity states. As a result, when data breaches are factored into the analysis, low-capacity states achieve higher scores,

whereas their scores decrease when data breaches are excluded from the MPI calculation. Additional details on these MPI results are presented in Appendix C.

The findings from this MPI assessment suggest that larger patient populations in high-capacity and mid-capacity states increase their exposure to cyber threats, making their healthcare systems more vulnerable to data breaches. With more patients, these states must manage higher volumes of EHR, expanding the attack landscape for potential cyber threats. The greater number of data transactions, system access points, and information-sharing activities inherently create more opportunities for human error. Additionally, larger healthcare systems often rely on complex networks of hospitals, clinics, and third-party vendors, increasing the risk of unauthorized access and security breaches. The higher demand for healthcare services in these states may also lead to resource constraints in cybersecurity investments, further exacerbating vulnerabilities. As a result, high-capacity and mid-capacity states face greater challenges in maintaining data privacy and mitigating cyber risks compared to low-capacity states with smaller patient populations.

Despite high-capacity and mid-capacity states investing in IT security systems, these investments appear insufficient, as they continue to experience vulnerabilities that cyber attackers exploit. The complexity of their healthcare networks, the volume of patient data, and the frequent exchange of information among hospitals, and third-parties create persistent security gaps. These factors make it difficult to fully safeguard patient data, even with increased financial resources.

In contrast, low-capacity states seem to have found a better balance between adopting EHR technology advancements and implementing effective data protection measures. With smaller patient populations and less complex healthcare infrastructures, these states may have more manageable IT environments, reducing vulnerability points in their security systems. Their ability to integrate privacy safeguards more effectively has likely contributed to fewer data breaches, ensuring stronger patient data protection and enhancing trust in healthcare services. Over time, this balance has led to secure and efficient information systems and enhanced performance.

As suggested in Section 2.4.1 of Essay 1, dividing the low-capacity states into two sub-groups may help address the high standard deviation observed within this category (as shown in Table 24), which reflects considerable variability in key performance and structural characteristics. This heterogeneity within the group could be distorting the MPI results. By dividing the low-capacity group into more homogeneous sub-groups, can improve the reliability of the MPI efficiency scores, and yield more accurate findings related to the increase in the overall productivity performance of the healthcare sector, and actionable insights for policy and resource allocation decisions.

The year by year MPI results in Table 25 reveal several interesting observations. The increase in MPI from 2009 to 2012 reflects the federal government's commitment to investing in incentive programs that supported healthcare providers in adopting EHR technology. In contrast, the decline in MPI from 2019 to 2021 coincides with the COVID-19 pandemic, which placed unprecedented strain on the U.S. healthcare services and severely impacted public health. However, the 2021-2022 period marks a strong recovery, driven by the introduction of vaccines. This led to reduction in hospital admissions, shorter patient stays, and lower mortality rates, ultimately alleviating the pressures that had overwhelmed the healthcare sector during the pandemic.

MPI Years	Meta (All States)	High-Capacity States	Mid-Capacity States	Low-Capacity States
2009-2010	0.716	0.006	0.786	0.825
2010-2011	0.948	0.806	0.782	1.010
2011-2012	1.063	0.692	0.890	0.947
2012-2013	0.926	0.752	0.866	0.939
2013-2014	0.867	0.803	0.804	0.877
2014-2015	0.949	0.820	0.904	0.964
2015-2016	0.931	1.022	0.810	0.922
2016-2017	0.940	0.866	0.992	0.929
2017-2018	0.983	0.984	0.944	0.996
2018-2019	0.935	0.953	0.931	0.930
2019-2020	0.930	0.695	0.887	0.964
2020-2021	0.665	0.820	0.712	0.649
2021-2022	3.384	1.152	1.045	4.221
Avg Change (2009-2022)	**1.095**	**0.798**	**0.873**	**1.167**

Table 25: MPI Results by Year for State Clusters (2009-2022)

ANOVA test was used to determine the difference in the MPI results from the three state clusters. Table 26 provides the statistics details about the ANOVA results. To test the hypothesis, the independent variable (categorical value) was represented by the three state clusters: high-capacity; mid-capacity; and low-capacity states; while the dependent variable was the MPI results, used to assess the potential impact of these clusters. Prior to running the ANOVA test, a Levene's test for homogeneity of variances was performed to confirm the equality of variances.

ANOVA TEST

State Clusters	N	Mean	SD	Std Error	DF	F Ratio	P-Value	Levene Test
High-Capacity	39	0.87292	0.251193	0.68697				
Mid-Capacity	143	0.94224	0.586095	0.35876				
Low-Capacity	481	1.17331	5.019991	0.19561				
p > 0.05					660	0.2209	0.8018	0.6348

Table 26: ANOVA Results - Hypothesis Testing

The ANOVA results do not support the hypothesis, yielding a p-value of 0.8018, indicating no statistically significant difference in MPI among the high-capacity, mid-capacity, and low-capacity state groups. Consequently, the Null Hypothesis (H_0) could not be rejected. There is no sufficient statistical evidence to conclude that the MPI differs significantly among high-capacity, mid-capacity, and low-capacity state clusters. This suggests that the classification into high, mid, and low capacity states does not have a meaningful impact on their MPI performance, implying that other factors might be driving productivity and efficiency changes in these DMUs. Finally, the low-capacity DMUs exhibited the highest mean MPI (1.173 ± 5.019), followed by mid-capacity states (0.9422 ± 0.586) and high-capacity states (0.873± 0.251).

Tables 27 and 28 presents the regression results for the three state clusters using two different dependent variables: Compromised Patient Records, and Monetary Penalties.

Regression Test- Compromised Patient Records (IV)

State Clusters	N	Mean	Sum of Square	DF	F Ratio	T-Ratio	P-Value
High-Capacity	39	0.8336	0.0563	38	0.8359	0.91	0.3665
Mid-Capacity	143	0.9298	0.0972	142	0.2766	-0.53	0.5998
Low-Capacity	481	1.166911	0.2776	480	0.011	-0.1	0.9166

$p > 0.05$

Table 27: Regression Results - Hypothesis Testing for State Clusters with MPI as the Dependent Variable and Compromised Patient Records as the Independent Variable

Regression Test- Monetary Penalties (IV)

State Clusters	N	Mean	Sum of Square	DF	F Ratio	T-Ratio	P-Value
High-Capacity	39	0.8336	0.075	38	1.1234	1.06	0.2961
Mid-Capacity	143	0.9248	0.00031	142	0.0009	0.03	0.9762
Low-Capacity	481	1.166911	0.1866	480	0.0074	-0.09	0.9315

$p > 0.05$

Table 28: Regression Results - Hypothesis Testing for State Clusters with MPI as the Dependent Variable and Monetary Penalties from HIPAA Violation as the Independent Variable

For these models, results from the regression analysis do not support the hypothesis for the two tested relationships. First, the relationship between compromised patient records and the DMUs productivity performance is represented by the calculated MPI for each state cluster. Second, the relationship is between the monetary penalties paid by each state cluster and their calculated MPI. As shown in Table 27, for the first relationship, the p values ranged from 0.3665 for high-capacity states to 0.9166 for the low-capacity states, indicating no statistically significant relationship between compromised patient records and MPI across the three state clusters.

Similarly for the second relationship, Table 28 shows that for monetary penalties and MPI productivity performance, the p values ranged from 0.2961 for high-capacity states and 0.9315 for the low-capacity states. As a result, the Null Hypothesis (H_0) could not be rejected for either relationship. These results suggest that data breaches and the number of compromised patient records do not appear to significantly impact the productivity performance of the state clusters. Simultaneously, monetary penalties paid by state clusters for data breaches do not have a significant effect on their productivity performance. In contrast, findings from the semi-structured interviews with SMEs indicated a consensus that compromised patient records and monetary penalties influence the productivity performance of state healthcare systems.

3.6 Limitation

Semi-structured interviews with SMEs were introduced to compensate for the limited amount of data in the literature related to the application of STS principles to solve human error challenges in IT. The interviews helped bridge this gap by providing valuable insights, knowledge depth, and increased confidence to the dissertation topic.

However, the interviews were time-consuming, labor intensive, and required a quite amount of planning. The process of setting up the interviews, preparing and conducting them, and analyzing the results was neither quick nor easy. Coordinating the interview sessions was challenging as well. In most cases, SMEs would not necessarily volunteer their time to provide their views for a session unless the interviewer had an existing relationship, or a prior connection with the SME through other means. The post interview process also involved analyzing a huge volume of notes from eight SMEs sessions, requiring significant time to document, transcribe, and synthetize them into a usable product to inform the dissertation.

3.7 Conclusion, Future Work, and Recommendation

Despite privacy concerns resulting from human error data breaches, the productivity performance of the DMUs has increased since 2009. Results from the MPI model show that, despite declines in productivity among high-capacity and mid-capacity states, significant gains in low-capacity states have more than compensated for these losses, resulting in an overall increase in healthcare sector productivity over time. It highlights the significance of the role of digital platforms in healthcare positively influencing the productivity performance in the sector despite unintended consequences, resulting from the persistent and complexity occurrences of human error data breaches.

The findings also reveal that when the “Data Breach Incidents” input variable was removed from the MPI analysis led to an increase in the MPI for the high-capacity and mid-capacity states, while the MPI for the low-capacity states declined. This finding suggests that data breach challenges impact influence productivity scores. However, the analysis found no statistically significant relationship between compromised patient records and MPI across the three state clusters.

These findings suggest that larger population of patients in high-capacity and mid-capacity states make their healthcare systems more vulnerable to cyberattacks. Investments in their IT security systems seem insufficient, as they continue to face vulnerabilities that cyber attackers continue to exploit. In contrast, low-capacity states appear to have effectively balanced EHR technology advancements with measures to address information privacy concerns, ultimately leading to improved patient care services over time.

ANOVA test results also indicate that no statistically significant difference exists in MPI among the high-capacity, mid-capacity, and low-capacity state clusters. Additionally, regression analyses revealed a weak relationship between compromised patient records and monetary penalties predictors, and the MPI across all state categories. Thus, further research is recommended in order to understand other socio-economic and demographic variables such as age distribution, education level, and population density can influence the productivity performance of healthcare provider from these state groups.

The increasing frequency of data breaches in healthcare systems raises critical concerns about patient safety and care quality. When patient records are compromised, there is a risk of erroneous information being introduced into EHR. Such erroneous information can lead to incorrect diagnoses, inappropriate treatments, and ultimately, increased mortality rates. Furthermore, the aftermath of data breaches often necessitates the implementation of additional security measures and system fixes, which can disrupt clinical workflows and divert resources away from patient care. Thus, further research is recommended to study the impact of data breaches on healthcare outcomes. Specifically, conduct an analysis of the relationship between compromised patient records and mortality rates.

Future studies should also explore the impact of modeling Managed Patients as an environmental variable in the Malmquist Productivity Index (MPI) when assessing the productivity of state healthcare systems. Since patient volume is largely determined by external factors such as population size and public health demands, conditions beyond

the control of individual systems, treating it as an input variable may impact efficiency scores and unfairly disadvantage high-demand states. Incorporating Managed Patients as a non-discretionary, environmental factor can lead to more accurate benchmarking by adjusting for contextual differences and better isolating true operational inefficiencies.

Recommendation

The findings from the MPI analysis in this chapter indicate that removing the “Data Breach Incidents” input variable changed the productivity of the state clusters, suggesting that data breach challenges impact the productivity performance of DMUs. Larger patient populations increase the exposure to cyber threats, making healthcare systems more vulnerable to data breaches.

To mitigate the impact of unintended consequences, such as information privacy concerns resulting from technology adoption, healthcare organizations should implement proactive measures. The following recommendations can help reduce the impact of data breach incidents and improve the productivity of DMUs:

- Annual Information Security Audits: Healthcare organizations should adopt regular security audits, similar to financial audits for large corporations, to ensure their systems effectively protect patient health information and prevent recurring breaches.
- Mandatory Malpractice Insurance: Healthcare entities must carry an information security malpractice insurance, specifically covering incidents where patient privacy is compromised due to human-error negligence, or system security failures. It should adopt regular security audits, similar to financial audits for large corporations, to ensure their systems effectively protect patient health information and prevent recurring breaches.

Insights from SMEs gathered through semi-structured interviews, combined with findings from the literature review, shape these recommendations to improve the productivity of state healthcare systems. This is achieved by implementing these

proactive business process measures, strengthening user awareness practices, and adopting measures to prevent or mitigate data breaches that could compromise patient records and heighten information privacy concerns related to technology adoption.

3.8 References

[1] Alder-Milstein, J., Everson, J., (2015). EHR Adoption and Hospital Performance: Time-Related Effects. Health Services Research.

[2] Althin, R., (2001). Measurement of Productivity Changes: Two Malmquist Index Approaches. Journal of Productivity Analysis.

[3] Appari, A., Johnson, E.M., Anthony, D.L., (2013). Meaningful Use of Electronic Health Records Systems and Process Quality of Care: Evidence from a Panel Data Analysis of U.S. Acute Care Hospitals. Health Service Res.

[4] Atasoy,H., Greenwood, B.N., McCullough, J.S., (2019). The Digitization of Patient Care: A Review of the Effects of Electronic Health Records on Health Care Quality and Utilization. Annual Review of Public Health.

[5] Barati, M., Yankson, B., (2022). Predicting the Occurrence of a Data Breach. International Journal of Information Management Data Insights.

[6] Bassem, B.S., (2014). Total Factor Productivity Change of MENA Microfinance Institutions: A Malmquist Productivity Index Approach. Scopus Elsevier.

[7] Belanger, F., Crossler, R.E., (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly.

[8] Blaya, J.A., Shin, S.S., Yagui, M.J., Yale, G., Suarez, C.Z., Asencios, L.L., (2007). AWe-Based Laboratory Information System to Improve Quality of Care of Tuberculosis Patients in Peru: Functional Requirements, Implementation and Usage Statistics. Bio-Medical Central –Medical Information Decision Making.

[9] Bowman, S., (2013). Impact of Electronic Health Record Systems on Information Integrity: Quality and Safety Implications. AHIMA.

[10] Bryans, J., (2006). Budi Arief. Security Implications of Structure. University of Newcastle.

[11] Department of Health and Human Services Federal Register, (2009). Office of National Coordinator for Health Information Technology.

[12] DHHS Office of Civil Rights, (2018). Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance. Health IT.Gov.

[13] DHHS Office of the National Coordinator (ONC) for Health Information Technology, (2022). National Electronic Health Records Survey - Non-Federal Acute Care Hospital IT Adoption and Use. Health IT.Gov.

[14] DHHS Office of the National Coordinator (ONC) for Health Information Technology, (2022). National Electronic Health Records Survey - Office-Based Physician IT Adoption and Use. Health IT.Gov.

[15] Dyson, R.G., Allen, R., Camanho, A.S., Podinovski, V.V., Sarrico, C.S., Shale, E.A., (2001). Pitfalls and Protocols in DEA. Elsevier.

[16] Emami-Mehrgani, B., Neumann, W. P., Nadeau, S., Bazrafshan, M., (2016). Considering Human Error in Optimizing Production and Corrective and Preventive Maintenance Policies for Manufacturing Systems. Scopus Elsevier.

[17] Esmaeilzadeh, P., (2020). How Does IT Identity Affect Individuals' Use Behaviors Associated With Personal Health Devices? An empirical study. Scopus Elsevier.

[18] Färe, R., Grosskopf, S., Norris, M., Zhankg, Z., (1994). Productivity Growth, Technical Progress, and Efficiency Change in Industrialized Countries. American Economic Association.

[19] Fineberg, H.V., (2012). A Successful and Sustainable Health System – How to Get There from Here. The New England Journal of Medicine.

[20] Freeman, W.J., Weiss, A.J., Heslin, K.C., (2018). Overview of U.S. Hospital Stays in 2016: Variation by Geographic Region. Agency for Healthcare Research and Quality.

[21] Hatch, B., Tillotson, C., Angier, H., Marino, M., Hoopes, M., Hughet, N., DeVoe, J., (2016). Using the Electronic Health Record for Assessment of Health Insurance in Community Health Centers. Oxford University Press.

[22] Health Insurance Portability and Accountability Act (HIPAA), (2021). Guide to Privacy and Security of Health Information. Department of Health and Human Services- Health IT.Gov.

[23] Huerta, T.R., Thompson, M.A., Ford, E.W., Ford, W.F., (2012). Electronic Health Record Implementation and Hospitals' Total Factor Productivity. Elsevier.

[24] Huguenin, J.M., (2012). Data Envelopment Analysis (DEA) - A Pedagogical Guide for Decision Makers in the Public Sector. IDHEAP.

[25] Kazley, A.S., Diana, M.L., Ford, E.W., Menachemi, N., (2012). Is Electronic Health Record Use Associated with Patient Satisfaction in Hospitals? Health Care Management Review.

[26] Khanijahani, A., Lezadi, S., Agoglia, S., Barber, S., Cox, C., Olivo, N., (2022). Factors Associated with Information Breach in Healthcare Facilities: A Systematic Literature Review. Journal of Medical Systems.

[27] Kisekka, V., Giboney, J.S., (2018). The Effectiveness of Health Care Information Technologies: Evaluation of Trust, Security Beliefs, and Privacy as Determinants of Health Care Outcomes. Journal of Medial Internet Research.

[28] Lee, C.C., Kim, Y., Choi, J.H., Porter, E.,(2022). Does Electronic Health Records Systems Implementation Hospital Efficiency, Profitability, and Quality? Journal of Applied Business and Economics.

[29] Mathews, K., (2018). HIPAA Compliance and the HITECH Act in 2018. Health IT. GOV.

[30] Milligan, F.J., (2006). Establishing a Culture for Patient Safety- The Role of Education. Scopus Elsevier.

[31] Mostoli, N., Rostamy, M., Shahverani, A., Behzadi, M.H., (2019). Using the Malmquist Index in Evaluation Process to Enhance Mathematical Literacy in High School Students. International Journal of Assessment Tools in Education.

[32] Ponemon Institute, (2024). Cost of a Data Breach Report. International Business Machines (IBM)-Security Report.

[33] Ponemon Institute, (2022). Cost of a Data Breach Report. International Business Machines (IBM)-Security Report.

[34] She, A.H., Zarour, M., Alenezi, M., Sarkar, A.K., Agrawal, A., Kumar, R., Khan, R.A., (2020). Healthcare Data Breaches: Insights and Implications. MDPI.

[35] Tran, P., (2021). Are Cybersecurity Issues Delaying Healthcare AI Adoption? Ferrum, Domain Knowledge.

[36] Upadhyay, S., Hu, H.F., (2021). A Qualitative Analysis of the Impact of Electronic Health Records (EHR) on Healthcare Quality and Safety: Clinicians' Lived Experiences. SAGE.

[37] Wang, Y.M., Lan, Y.X., (2011). Measuring Malmquist Productivity Index: A New Approach Based on Double Frontiers Data Envelopment Analysis.

[38] Wikina, S.B., (2014). What Caused the Breach? An Examination of Use of Information Technology and Health Data Breaches. National Institute of Health.

[39] Wilkinson, F., (2022). Industrial Revolution & Technology. National Geographic Society.

[40] Yarovenko, H., Kuzmenko, O., Stumpo, M., (2020). DEA – Analysis of the Effectiveness of the Country's Information Security System. ARMG Publishing.

[41] Yasnoff, W.A., (2016). A Secure and Efficiently Searchable Health Information Architecture. Scopus Elsevier.

[42] Zhao, R., (2018). Technology and Economic Growth: From Robert Solow to Paul Romer. Wiley.

[43] Zimy, G., Yannick, S., Hongzhong, Z., Thierry, B., (2016). Technical Efficiency Assessment Using Data Envelopment Analysis: An Application to the Banking Sector of Cote d'Ivoire. Scopus Elsevier.

Appendix B

Comparison of Average Productivities (2009-2022) for All States vs. State Clusters

Meta (All States) DMU	Malmquist Productivity Index	Efficiency Change	Technological Change	Pure Output Efficiency Change	Output Scale Efficiency Change
Alabama	0.965298	1.049425	0.928041	0.996019	1.052049
Alaska	9.325433	1.000000	9.325433	1.000000	1.000000
Arizona	0.921455	1.014692	0.918765	1.006752	1.005592
Arkansas	0.915731	0.996911	0.924468	0.994979	0.999861
California	0.819558	1.052894	0.834691	1.000795	1.053417
Colorado	0.896906	0.996249	0.920821	1.002114	0.996113
Connecticut	0.957594	1.053460	0.919598	0.999990	1.053742
Delaware	0.883788	1.000000	0.883788	1.000000	1.000000
District of Columbia	0.939360	1.000000	0.939360	1.000000	1.000000
Florida	0.883292	1.042394	0.878328	1.011086	1.033690
Georgia	0.885597	1.010829	0.851040	0.982663	1.023527
Hawaii	0.947398	1.000000	0.947398	1.000000	1.000000
Idaho	0.884249	1.000000	0.884249	1.000000	1.000000
Illinois	0.859113	1.023473	0.898999	0.998010	1.025639
Indiana	0.859288	0.983239	0.902943	0.998862	0.982272
Iowa	1.143833	1.212835	0.937657	0.998920	1.207711
Kansas	0.947440	0.999949	0.951882	0.999750	0.999772
Kentucky	0.943421	1.046452	0.910304	0.997957	1.048007
Louisiana	0.880588	0.997302	0.882362	0.997504	0.999726
Maine	0.994749	1.032758	0.979629	0.999313	1.031655
Maryland	0.878364	0.991620	0.899484	0.999973	0.994902
Massachusetts	0.874490	1.017914	0.884552	1.001780	1.017445
Michigan	0.883690	1.008560	0.916060	1.000458	1.004093
Minnesota	0.901283	1.004705	0.921460	0.997205	1.009349
Mississippi	0.917772	0.986607	0.927923	0.998686	0.988141
Missouri	0.860744	1.022405	0.895002	1.001102	1.022251
Montana	0.869667	1.003714	0.848486	1.000144	1.003274
Nebraska	0.958508	1.013682	0.954886	0.999910	1.013625
Nevada	0.907739	1.000000	0.907739	1.000000	1.000000
New Hampshire	0.898625	1.007450	0.892866	0.998931	1.008110
New Jersey	0.882434	0.989788	0.902085	1.003740	0.985184
New Mexico	0.894246	1.001128	0.890525	1.000007	1.001058
New York	0.837467	1.000180	0.869315	1.001817	0.991230
North Carolina	0.867213	1.012306	0.897361	1.004415	1.009131
North Dakota	0.977275	1.021420	0.962548	1.000240	1.021063
Ohio	0.833438	1.049155	0.859857	1.024494	1.043454
Oklahoma	0.959320	1.036411	0.916961	0.996011	1.040127
Oregon	0.865047	0.980723	0.881215	0.997769	0.982790
Pennsylvania	1.235156	1.450745	0.912882	0.988372	1.439326
Rhode Island	0.919946	1.000000	0.919946	1.000000	1.000000
South Carolina	0.865364	1.004402	0.872875	0.996241	1.000432
South Dakota	0.904040	1.026397	0.899943	0.999360	1.025843
Tennessee	0.867380	0.981324	0.908459	0.999932	0.982089
Texas	0.844016	1.076626	0.829366	1.004461	1.073388
Utah	1.124483	1.000000	1.124483	1.000000	1.000000
Vermont	0.878681	1.000000	0.878681	1.000000	1.000000
Virginia	0.971355	1.085452	0.908699	1.007188	1.067985
Washington	0.996970	1.129866	0.911291	1.003178	1.130746
West Virginia	0.939377	1.008907	0.938909	0.995522	1.013109
Wisconsin	1.075035	1.208208	0.923037	1.001431	1.196558
Wyoming	1.306293	1.000000	1.306293	1.000000	1.000000
Grand Total	*1.095088*	*1.032011*	*1.082019*	*1.000139*	*1.030931*

High-Capacity States DMU	Malmquist Productivity Index	Efficiency Change	Technological Change	Pure Output Efficiency Change	Output Scale Efficiency Change
California	0.808239	1.000000	0.808239	1.000000	1.000000
New York	0.778680	1.000000	0.778680	1.000000	1.000000
Texas	0.806687	1.000000	0.806687	1.000000	1.000000
Grand Total	*0.797869*	*1.000000*	*0.797869*	*1.000000*	*1.000000*

Mid-Capacity States DMU	Malmquist Productivity Index	Efficiency Change	Technological Change	Pure Output Efficiency Change	Output Scale Efficiency Change
Florida	0.906663	1.012069	0.897351	1.007589	1.002591
Georgia	0.834638	1.000110	0.833273	1.000000	1.000110
Illinois	0.870960	1.012304	0.865798	1.000249	1.011034
Massachusetts	0.923065	1.004980	0.924734	1.000000	1.004980
Michigan	0.864283	0.999899	0.867511	0.999279	0.998601
New Jersey	0.875787	1.000000	0.875787	1.000000	1.000000
North Carolina	0.862054	1.007359	0.857356	1.007443	1.000242
Ohio	0.876243	1.026883	0.862014	1.018865	1.013226
Pennsylvania	0.882682	1.032804	0.868241	0.994444	1.030089
Virginia	0.797444	1.000729	0.792988	1.000452	1.000117
Washington	0.912748	1.000000	0.912748	1.000000	1.000000
Grand Total	***0.873324***	***1.008831***	***0.868891***	***1.002575***	***1.005545***

Low-Capacity States DMU	Malmquist Productivity Index	Efficiency Change	Technological Change	Pure Output Efficiency Change	Output Scale Efficiency Change
Alabama	0.966990	1.049425	0.928906	0.996019	1.052049
Alaska	9.325433	1.000000	9.325433	1.000000	1.000000
Arizona	0.921455	1.014692	0.918765	1.006752	1.005592
Arkansas	***0.915731***	***0.996911***	***0.924468***	***0.994979***	***0.999861***
Colorado	0.896906	0.996249	0.920821	1.002487	0.996059
Connecticut	0.957594	1.053460	0.919598	1.000062	1.053742
Delaware	0.883788	1.000000	0.883788	1.000000	1.000000
District of Columbia	0.939360	1.000000	0.939360	1.000000	1.000000
Hawaii	0.947398	1.000000	0.947398	1.000000	1.000000
Idaho	0.884249	1.000000	0.884249	1.000000	1.000000
Indiana	0.859278	0.983217	0.902968	0.998812	0.982272
Iowa	1.143833	1.212835	0.937657	0.998920	1.207711
Kansas	0.947440	0.999949	0.951882	0.999750	0.999772
Kentucky	0.944836	1.046452	0.910930	0.997957	1.048007
Louisiana	0.880506	0.997302	0.882147	0.997504	0.999726
Maine	0.994749	1.032758	0.979629	0.999313	1.031655
Maryland	0.878364	0.991620	0.899484	0.999989	0.994842
Minnesota	0.901283	1.004705	0.921460	0.997602	1.009026
Mississippi	0.917772	0.986607	0.927923	0.998686	0.988141
Missouri	0.860744	1.022405	0.895002	1.001102	1.022251
Montana	0.869667	1.003714	0.848486	1.000144	1.003274
Nebraska	0.958508	1.013682	0.954886	0.999910	1.013625
Nevada	0.907739	1.000000	0.907739	1.000000	1.000000
New Hampshire	0.898625	1.007450	0.892866	0.998931	1.008110
New Mexico	0.894246	1.001128	0.890525	1.000007	1.001058
North Dakota	0.977275	1.021420	0.962548	1.000240	1.021063
Oklahoma	0.959464	1.036411	0.917034	0.996011	1.040127
Oregon	0.864796	0.980723	0.880778	0.997842	0.982673
Rhode Island	0.919946	1.000000	0.919946	1.000000	1.000000
South Carolina	0.865364	1.004402	0.872875	0.996241	1.000432
South Dakota	0.904040	1.026397	0.899943	0.999360	1.025843
Tennessee	0.867380	0.981324	0.908459	0.999932	0.982089
Utah	1.124483	1.000000	1.124483	1.000000	1.000000
Vermont	0.878681	1.000000	0.878681	1.000000	1.000000
West Virginia	0.939377	1.008907	0.938909	0.995522	1.013109
Wisconsin	1.080220	1.220644	0.923125	1.001987	1.196795
Wyoming	1.306293	1.000000	1.306293	1.000000	1.000000
Grand Total	***1.167130***	***1.018778***	***1.157553***	***0.999353***	***1.018349***

Appendix C

Sensitivity Analysis - Comparison of Average Productivities (2009-2022) for All States vs. State Clusters

Meta (All States) DMU	Malmquist Productivity Index	Efficiency Change	Technological Change	Pure Output Efficiency Change	Output Scale Efficiency Change
Alabama	0.912082	1.012804	0.918106	0.995990	1.017654
Alaska	0.941063	1.000000	0.941063	1.000000	1.000000
Arizona	0.936078	1.008905	0.939750	1.006683	1.003772
Arkansas	0.921767	1.005963	0.926873	0.994851	1.010392
California	0.882334	1.112134	0.842627	1.000795	1.112245
Colorado	0.923349	1.012620	0.930122	1.002111	1.013311
Connecticut	0.919426	1.048061	0.890757	0.999990	1.048160
Delaware	0.924726	1.000000	0.924726	1.000000	1.000000
District of Columbia	1.005460	1.000000	1.005460	1.000000	1.000000
Florida	0.945471	1.074324	0.903222	1.011066	1.065616
Georgia	0.853481	0.999802	0.884512	0.982663	1.017230
Hawaii	0.930237	1.000000	0.930237	1.000000	1.000000
Idaho	0.908187	1.004194	0.906833	1.000000	1.004194
Illinois	0.900168	1.051697	0.902540	0.998010	1.053900
Indiana	0.922862	1.038575	0.912406	0.998856	1.040798
Iowa	0.953129	1.040017	0.934661	0.998726	1.041263
Kansas	0.917945	1.032001	0.909062	0.999746	1.032325
Kentucky	0.881941	0.996595	0.893794	0.997947	0.999369
Louisiana	0.904191	1.005423	0.916804	0.997505	1.008316
Maine	0.905842	1.039808	0.884083	0.999280	1.040361
Maryland	0.900722	1.023506	0.889317	0.999936	1.021641
Massachusetts	0.942892	1.088677	0.890417	1.001781	1.087169
Michigan	0.897875	1.033673	0.903788	1.000375	1.031605
Minnesota	0.957128	1.050682	0.926901	0.997204	1.055752
Mississippi	0.917880	1.023962	0.910425	0.998686	1.025375
Missouri	0.911726	1.051274	0.896845	1.001092	1.049511
Montana	0.898654	1.004817	0.898290	1.000140	1.004369
Nebraska	0.914981	1.027143	0.905420	0.999909	1.027219
Nevada	0.917959	1.000000	0.917959	1.000000	1.000000
New Hampshire	0.884887	0.991510	0.896374	0.998932	0.992518
New Jersey	0.921484	1.041832	0.898138	1.003694	1.038108
New Mexico	0.892310	1.004822	0.889817	1.000015	1.004574
New York	0.904067	1.043052	0.891621	1.001818	1.037217
North Carolina	0.938082	1.064418	0.907556	1.004415	1.059372
North Dakota	0.913437	1.018530	0.902660	1.000240	1.018151
Ohio	0.917017	1.103858	0.872970	1.024494	1.084869
Oklahoma	0.898586	1.019017	0.896541	0.996012	1.023723
Oregon	0.858241	1.002758	0.870007	0.997767	1.004688
Pennsylvania	0.895082	1.037130	0.901660	0.988338	1.047077
Rhode Island	0.936357	1.000807	0.933522	1.000000	1.000807
South Carolina	0.893607	1.001773	0.907426	0.995267	1.006556
South Dakota	0.871183	0.970124	0.901118	0.999343	0.970679
Tennessee	0.908632	1.027322	0.910074	0.999932	1.027158
Texas	0.899890	1.135500	0.838155	1.004461	1.132428
Utah	1.124770	1.000000	1.124770	1.000000	1.000000
Vermont	0.922758	1.011898	0.914581	1.000000	1.011898
Virginia	0.933280	1.051039	0.897707	1.006896	1.044782
Washington	0.939401	1.054571	0.898378	1.003181	1.051807
West Virginia	0.858327	0.976785	0.880393	0.995523	0.980686
Wisconsin	0.955779	1.057747	0.916596	1.001357	1.055953
Wyoming	1.142794	1.000000	1.142794	1.000000	1.000000
Grand Total	*0.922736*	*1.027473*	*0.914311*	*1.000099*	*1.027541*

High-Capacity States DMU	Malmquist Productivity Index	Efficiency Change	Technological Change	Pure Output Efficiency Change	Output Scale Efficiency Change
California	0.894287	1.000000	0.894287	1.000000	1.000000
New York	0.894955	1.000000	0.894955	1.000000	1.000000
Texas	0.899347	1.000000	0.899347	1.000000	1.000000
Grand Total	*0.896196*	*1.000000*	*0.896196*	*1.000000*	*1.000000*

Mid-Capacity States DMU	Malmquist Productivity Index	Efficiency Change	Technological Change	Pure Output Efficiency Change	Output Scale Efficiency Change
Florida	0.921612	1.031075	0.897050	1.007132	1.023953
Georgia	0.847019	1.000110	0.845363	1.000000	1.000110
Illinois	0.880153	1.015016	0.876509	0.999213	1.016181
Massachusetts	0.948219	1.015263	0.940972	1.000000	1.015263
Michigan	0.888942	0.991105	0.902976	0.998863	0.990889
New Jersey	0.922648	1.000000	0.922648	1.000000	1.000000
North Carolina	0.892089	1.011743	0.884141	1.007437	1.004645
Ohio	0.895525	1.021979	0.889178	1.018871	1.007492
Pennsylvania	0.890804	0.989340	0.912337	0.994241	0.995388
Virginia	0.913454	1.002369	0.912480	1.000531	1.001666
Washington	0.935364	1.000000	0.935364	1.000000	1.000000
Grand Total	*0.903257*	*1.007091*	*0.901729*	*1.002390*	*1.005053*

Low-Capacity States DMU	Malmquist Productivity Index	Efficiency Change	Technological Change	Pure Output Efficiency Change	Output Scale Efficiency Change
Alabama	0.912082	1.012804	0.918106	0.995990	1.017654
Alaska	0.941063	1.000000	0.941063	1.000000	1.000000
Arizona	0.936078	1.008905	0.939750	1.006683	1.003772
Arkansas	*0.921767*	*1.005963*	*0.926873*	*0.994851*	*1.010392*
Colorado	0.923349	1.012620	0.930122	1.002481	1.013146
Connecticut	0.919426	1.048061	0.890757	1.000062	1.048161
Delaware	0.924726	1.000000	0.924726	1.000000	1.000000
District of Columbia	1.005460	1.000000	1.005460	1.000000	1.000000
Hawaii	0.930237	1.000000	0.930237	1.000000	1.000000
Idaho	0.908187	1.004194	0.906833	1.000000	1.004194
Indiana	0.922862	1.038575	0.912406	0.998806	1.040864
Iowa	0.953129	1.040017	0.934661	0.998726	1.041263
Kansas	0.917945	1.032001	0.909062	0.999746	1.032325
Kentucky	0.881941	0.996595	0.893794	0.997947	0.999369
Louisiana	0.904191	1.005423	0.916804	0.997505	1.008316
Maine	0.905842	1.039808	0.884083	0.999280	1.040361
Maryland	0.900722	1.023506	0.889317	0.999957	1.021621
Minnesota	0.957128	1.050682	0.926901	0.997601	1.055461
Mississippi	0.917880	1.023962	0.910425	0.998686	1.025375
Missouri	0.911726	1.051274	0.896845	1.001092	1.049511
Montana	0.898654	1.004817	0.898290	1.000140	1.004369
Nebraska	0.914981	1.027143	0.905420	0.999909	1.027219
Nevada	0.917959	1.000000	0.917959	1.000000	1.000000
New Hampshire	0.884887	0.991510	0.896374	0.998932	0.992518
New Mexico	0.892310	1.004822	0.889817	1.000015	1.004574
North Dakota	0.913437	1.018530	0.902660	1.000240	1.018151
Oklahoma	0.898586	1.019017	0.896541	0.996012	1.023723
Oregon	0.858241	1.002758	0.870007	0.997840	1.004558
Rhode Island	0.936357	1.000807	0.933522	1.000000	1.000807
South Carolina	0.893607	1.001773	0.907426	0.995267	1.006556
South Dakota	0.871183	0.970124	0.901118	0.999343	0.970679
Tennessee	0.908632	1.027322	0.910074	0.999932	1.027158
Utah	1.124770	1.000000	1.124770	1.000000	1.000000
Vermont	0.922758	1.011898	0.914581	1.000000	1.011898
West Virginia	0.858327	0.976785	0.880393	0.995523	0.980686
Wisconsin	0.955779	1.057747	0.916596	1.001762	1.055494
Wyoming	1.142794	1.000000	1.142794	1.000000	1.000000
Grand Total	*0.926730*	*1.013769*	*0.924232*	*0.999306*	*1.014599*

Chapter 4.0 - Essay 3: Enhanced Reason's Resiliency Model to Reduce Human Error Data Breaches - Application of Policy as a Safeguard Layer to Patient Record Breaches

"There's no silver bullet with cybersecurity; a layered defense is the only viable option." James Scott.

Abstract

HIPAA and its subsequent amendments made an impact in past years on the operation of healthcare organizations providing safeguards to protect EHR systems. However, the U.S healthcare industry continues to operate under this law that was enacted about three decades ago. As technology continues to advance at a rapid pace along with consumers playing a greater role in the management of their healthcare through digital health, the privacy guidance provided by HIPAA to protect patient privacy should also have shifted to reflect the new reality (Theodos, 2020).

Monetary penalties are no longer sufficient in decreasing the number of compromised patient records within the healthcare sector (Theodos, 2020). Patient privacy continues to be a crucial issue in healthcare information security. Although the literature underscores the advantages of adopting EHR technology to enhance healthcare service quality, it also highlights information security as one of the sector's most pressing challenges. HIPAA monetary penalties have been used as a regulatory tool to enforce compliance with privacy and security standards and reduce data breaches.

This chapter presents an enhanced Reason's Resiliency Model by integrating a STS management framework into its layered approach to mitigate human error challenges in healthcare information security. The enhanced model serves as a platform for evaluating policy compliance, represented by HIPAA monetary penalties, as a safeguard layer aimed at reducing patient record breaches caused by human-technology interface errors.

The findings indicate that monetary penalties for HIPAA violations have not been effective in reducing the number of compromised patient records in healthcare.

KEYWORDS: HIPAA, Monetary Penalties, Reason's Resiliency Model, Socio-Technical Systems (STS)

4.1 Introduction

Essay 3 aims to enhance Reason's Resiliency Model by integrating an STS management framework into its layered approach to addressing human error challenges in healthcare information security. The enhanced model is utilized to evaluate the effectiveness of the HIPAA policy as a security safeguard designed to reduce the occurrence of successful data breaches and the compromise of patient healthcare records.

HIPAA monetary penalties serve as a regulatory enforcement tool to mitigate data breaches in healthcare by promoting compliance with privacy and security standards. Government uses policies to address persistent issues or to achieve specific objectives.

Congress enacted HIPAA in 1996 with the original intention of reforming the health insurance market and improving the productivity and effectiveness of the healthcare system (HIPAA Journal, 2022). Other provisions added to the original HIPAA require the DHHS to adopt national standards for electronic health care transactions, and enforce federal privacy protections for individually identifiable health information (DHHS OCR Privacy Rule, 2022). Compliance with HIPPA regulations is mandatory for healthcare providers, health plans, business associates, and healthcare clearinghouses.

Congress introduced the Privacy Rule under HIPAA in 2003 to regulate the use and disclosure of protected health information (PHI), and set standards for healthcare organizations to protect the privacy of patient medical information. It also included standards for privacy rights of individuals to understand and control how their health information is used. To date, continuous enforcement of this provision has been a driving force behind the organizations' protocols for prevention, detection, and remediation of reported incidents and unauthorized disclosures of PHI (DHHS OCR Privacy Rule, 2022).

The Security Rule of 2005 and the Omnibus Rule of 2013 are other HIPAA provisions that have contributed to the protection of patient records. The Security Rule requires

entities to implement physical, technical, and administrative safeguards to protect the privacy of PHI. The Omnibus Rule stipulates that all breaches where electronic PHI compromising more than 500 records must be reported to the DHHS OCR (DHHS OCR Security Rule, 2022). As established by the HITECH Act of 2009, penalties for violations are also enforced by the DHHS OCR (Matthews, 2018).

Despite its challenges preventing data breaches in the sector, HIPAA remains the most critical enacted law related to healthcare privacy protection, as it provides a direct and unavoidable right to privacy for all patients (Theodos et al., 2020).

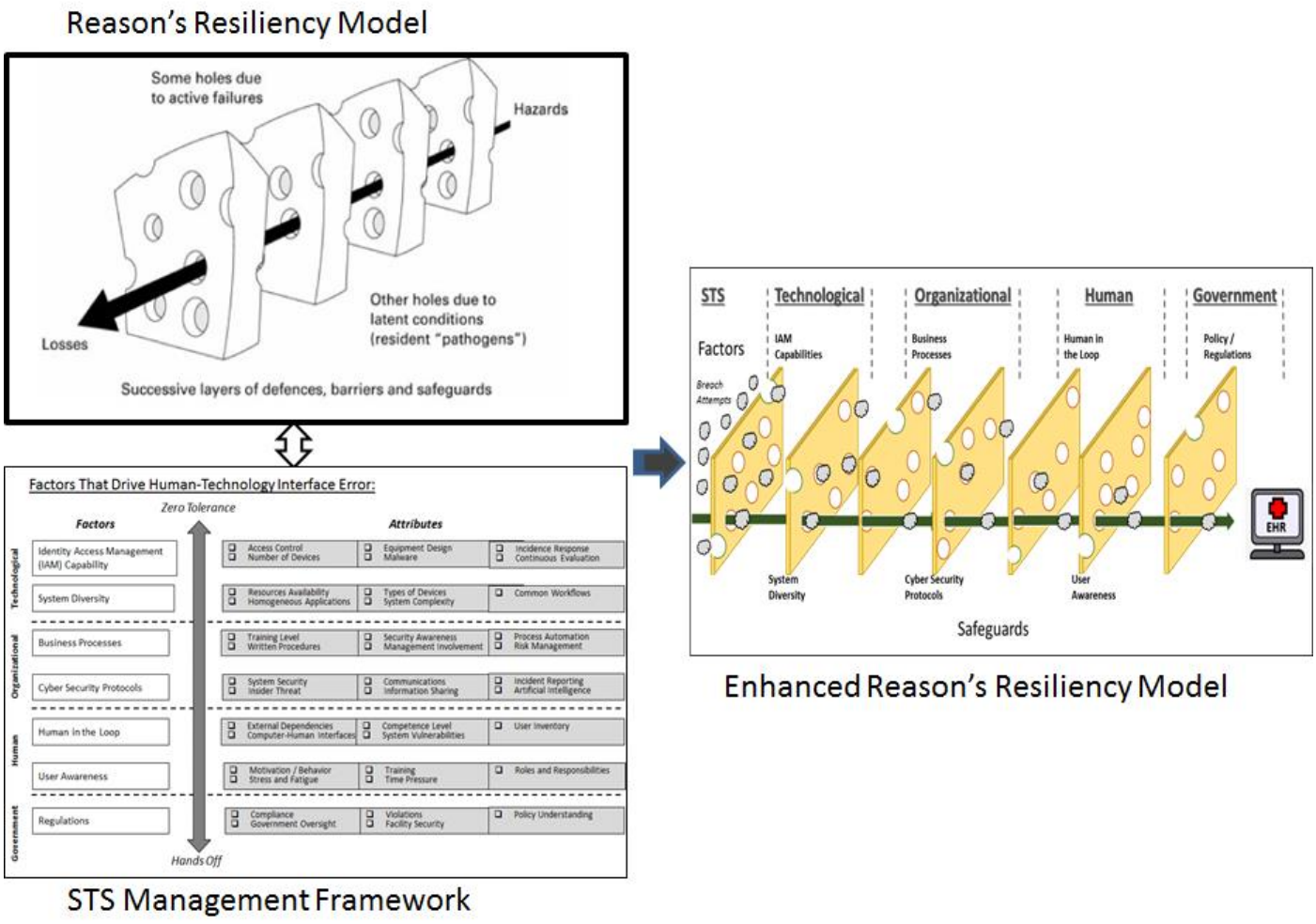


Figure 17: Integration of Reason's Resiliency Model and STS Management Framework Result in an Enhanced Reason's Resiliency Model to Improve Information Security Systems

Figure 17 presents an enhanced version of Reason's Resiliency Model, integrating an STS management framework (Figure 12) to strengthen its layered approach to addressing human error challenges in healthcare information security. This enhanced model builds upon the original framework (Figure 2) by incorporating government regulation, specifically HIPAA policy, as an additional safeguard against data breaches. In this essay, the updated model, Figure 18, is used to assess the effectiveness of HIPAA in preventing patient healthcare records from being compromised and mitigating the risk of security incidents.

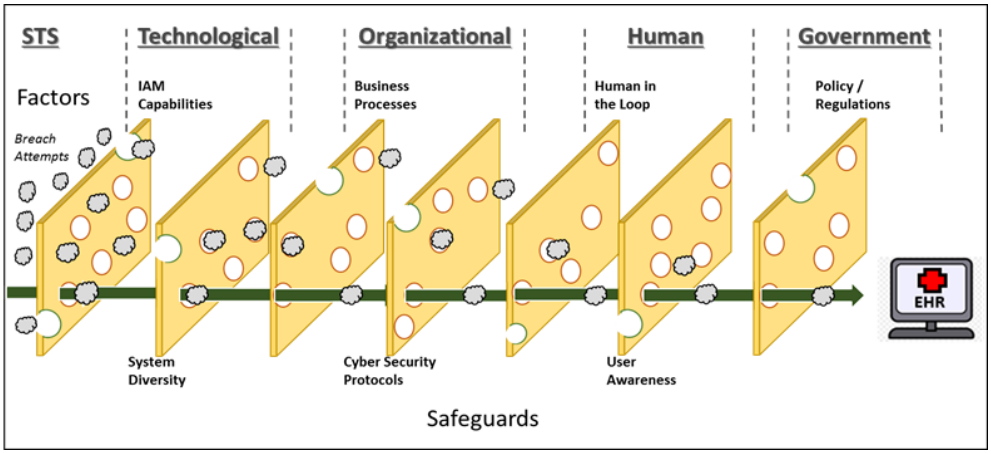


Figure 18: Enhanced Reason's Resiliency Model- Application of HIPAA Policy as a Safeguard Layer to Reduce Compromised Patient Records

In the application of this enhanced model (Perneger, 2005), each slice is a security safeguard (e.g. government policy), that has holes or imperfections (e.g. human-technology errors) allowing the hazard (data breach attempts) to progress, or blocking them from becoming an accident, or if all holes do line up, allowing a hazard to become an accident (compromised patient records). Assessing the impact of HIPAA policy as a security safeguard against human-technology interface errors can help organizations prioritize the development and enforcement of protections to safeguard data integrity, which is essential for maintaining patient trust.

The essay provides to the DHHS OCR policy makers, an improved understanding of the effectiveness of HIPAA in reducing compromised patient records. It also serves as a foundation for recommending policy changes to strengthen safeguards where data breaches occur most frequently.

4.2 Research Problem

The literature suggests that HIPAA requires modernization to address emerging challenges in healthcare information security. Experts argue that HIPPA and subsequent amendments made an impact in past years on the operation of healthcare organizations providing safeguards to protect EHR systems. However, the proliferation of digital health data, trends in data use, increased in the use of telehealth applications, and patient's accesses to their health records all have created new challenges (Theodos et al., 2020). As of December 2024, these challenges remained unaddressed by the existing HIPAA framework.

As the legal framework that protects the privacy of patient health information, the enforcement of HIPAA regulations could have a significant influence on how healthcare organizations handle and protect EHR data. Under HIPAA, reported non-compliances are submitted for investigation and final ruling determination with some of these investigations resulting in monetary penalties to the healthcare organizations.

Monetary penalties do not longer seem effective as deterrent to prevent violations to HIPAA laws (Theodos et al., 2020). The U.S healthcare industry continues to operate under a law that was enacted about three decades ago. Per the literature (Theodos et al., 2020), (Alder, 2021), as technology continues to advance at a rapid pace along with consumers playing a greater role in the management of their healthcare through digital health, the privacy guidance provided by federal law should also have shifted to reflect the new reality.

Essay 3 tests a hypothesis to evaluate the effectiveness of monetary penalties as deterrent against HIPAA violations and their impact on reducing compromised patient records, seeking to refute or confirm the findings from the literature. The hypothesis states, **HIPAA monetary penalties are positively correlated with a reduction in the number of compromised patient records.** To test the effectiveness of HIPAA policy in influencing the performance of the DMUs (States), a regression model was developed

using compromised patient records as the dependent variable, and monetary penalties as the independent variable.

The essay uses the enhanced Reason's Resiliency Model (Figure 18) to address the research question, **what is the effect of HIPAA policy compliance, as a security safeguard against errors that result as a consequence of the human-technology interface, on the performance of the states' information security systems?**

4.3 Technical Background

Understanding Reason's Theory of Accident Causation can help us design systems which are more resilient to failures, errors, and even security threats. The vast majority of catastrophes, such as plane crashes, are created by a series of factors that line up in just the wrong way, allowing seemingly-small details to add up to a major incident. Similarly in information security, a weak password could lead an attacker to move within the organization network identifying sensitive healthcare organization, and copying and transferring data out of a system that lacks sufficient monitoring tools or a security team that overlook or misinterpret intruders' access alerts (Schwartz, 2021).

In his 2000 "Human Error: Models and Management" paper, James Reason reports that, in a complex system such as healthcare, human error is likely to occur and that expecting perfection from imperfect human beings or punishing them for their mistakes will not improve safety. The model indicates that the preferred strategy is either to prevent an error from occurring or prevent the error from causing harm through the application of multiple steps that function as a safety net (Reason, 2000).

Reason's Resiliency model suggests that the easier solution to protect a system is to add more layers of safeguard, or additional component of redundancy, to protect a system. However, this approach could quickly become over complicated introducing technical challenges such as system latency, and add operational cost. A more practical approach is to analyze the system to determine if there may be a better way to address security concerns.

Reason's Resiliency Model is applied in risk management, particularly of human error in safety-critical systems like healthcare. HIPAA compliance involves a broad range of STS risks, including technical, administrative, physical, and human factors. Integrating the STS Management Framework with Reason's Resiliency Model aligns with the need for a holistic risk management approach, establishing a robust system of safeguards to enhance resilience against potential threats to EHR information security.

4.4 Research Method

4.4.1 Data

The comprehensive quantitative datasets, Table 29, with all reported cybersecurity incidents and compromised patient records, described in Chapters 2 and 3 are also used to support modeling and hypothesis testing for this chapter. An additional field has been incorporated to account for HIPAA violation monetary penalties imposed on the state healthcare systems (DMUs) for non-compliance with physical, technical, and/or administrative safeguard regulations. These penalties include civil monetary settlements, which range from $100 to $50,000 per violation, depending on the severity of the breach and the extent of harm caused to patients' PHI.

Data by State	Category	Range	Source
Data Breach Incidents	Information Security	2009-2024	DHHS- Office of Civil Rights
Patient Records Compromised	Information Security	2009-2024	DHHS- Office of Civil Rights
HIPAA Violations -Monetary Penalty Settlement	Information Security and Policy	2009-2024	DHHS- Office of Civil Rights

Table 29: Quantitative Datasets with Sources and Data Range Used in Essay 3

This essay employs a statistical analysis using regression with lagged explanatory variables. To facilitate this assessment, a Microsoft Excel database was created to track data breach incidents, compromised patient records, and HIPAA violation monetary penalties imposed on DMUs for non-compliance. The database spans events from 2009 to 2024 across all 50 states and the District of Columbia, categorizing each entry by the type of data breach, the number of records compromised, and, where applicable, the HIPAA monetary penalties issued for non-compliance.

To evaluate the impact of prior-year government HIPAA policy enforcement, the database includes multiple fields with one-year and two-year lagged variables. Given the extensive dataset covering the 2009-2024 period, an Excel pivot table was developed to systematically categorize and quantify incidents based on multiple parameters, enabling effective analysis. Table 30 outlines the database fields used for the regression analysis, supporting the development of multiple models to test the essay's hypothesis.

DMU	Year (t)	Compromised Patient Records (t) (Dep Variable)	Monetary Penalty (t-1) (Indep Var)	Monetary Penalty (t-2) (Indep Var)	Compromised Patient Records (t-1) (Indep Variable)	Compromised Patient Records (t-2) (Indep Variable)	Data Breaches (t) (Indep Var)
Alabama	2011	14,292	0	0	768	0	2
Alaska	2011	566	0	0	0	0	1
Arizona	2011	18,838	0	0	0	0	5
Arkansas	2011	4,588	0	0	0	0	2
California	2011	30,687	0	0	30,487	0	7
Colorado	2011	5,889	0	0	0	0	2
Connecticut	2011	1,631	250,000	0	9,674	0	1
Delaware	2011	0	0	0	0	0	0
District of Columbia	2011	0	0	0	0	3,800	0

Table 30: Quantitative Dataset of Breach Incidents and Monetary Penalties (2009-2024)

4.4.2 Approach

Previous studies found in the literature indicate that HIPAA violations typically take between nine to 12 months to reach settlement (Johnson, 2022). Thus, the research approach for this essay uses statistical regression analysis with one-year lagged response explanatory variables. One-year was applied as the lag order to the independent variables.

The primary regression model that was formulated, Equation (4), uses a multivariable approach incorporating two one-year lagged response explanatory variables. The dependent variable used in the model is compromised patient records (t), while the independent variables included one-year lagged monetary penalties (t-1) and compromised patient records (t-1). The lag structure enabled an evaluation of how HIPAA monetary penalties and compromised patient records in a given year (t-1) impact patient record breaches the following year (t).

$$PR_i^t = \int (MP_i^{t-1}, PR_i^{t-1}, ...) + \varepsilon_i^t$$ Equation (4)

i= State Healthcare System; t: Time in Years;

Dependent Variable:

PR_i^t = Compromised patient records by state i in year t,

Independent Variables:

MP_i^{t-1} = Monetary penalties paid by state i in year t-1,

PR_i^{t-1} = Compromised patient records by state i in year t-1,

Additionally, sensitivity analyses were conducted using two-year lagged (t-2) variables to further examine these relationships.

The hypothesis that is tested in this essay states that:

H3: HIPAA monetary penalties are positively correlated with a reduction in the number of compromised patient records.

4.5 Results and Discussion

Qualitative - Semi-Structured Interviews

Semi-structured interviews provided valuable insights from cybersecurity and healthcare professionals on nuances in patient care practices that were not evident in the literature. The interviews provided additional insights into the organizational impact of data breaches and the effectiveness of policy compliance in mitigating these incidents. Insights from these real world experts informed the variables selection for the regression models for Essay 3, which evaluate the effectiveness of HIPAA policy reducing the number of compromised patient records. Some organizations find that paying HIPAA monetary penalties is more cost-effective than investing in IT system corrections. The SMEs insight also revealed that government entities are prohibited from paying ransoms to cyber attackers, further complicating responses to cybersecurity threats in the healthcare sector.

Table 31 summarizes findings from the semi-structured interviews applicable to Essay 3, including takeaways, qualitative results, and how the findings inform this dissertation. Additional details are also included in Appendices F thru J at the end of the dissertation.

Literature Gap	Interviews Takeaway	Interview Findings	Qualitative Results	How Findings Inform the Research
Essay 3: Confirm or Refute the Effectiveness of HIPAA Policy on Healthcare Performance	Monetary penalties to state healthcare systems for HIPAA non-compliances are not severe enough	Policy influences management behavior to improve IT security • Improves users awareness • Leads to management involvement • Improves cooperation from business partners • Introduces need for data protection training Mixed results about effectiveness of monetary penalties • Comply to maintain patients' trust • Policy sometimes work on protecting data • Data breaches continue to flood the sector Best practices to strengthen compliance • Improve policy provisions • Introduce user training • Create needs of policy enforcement • Increase severity in compliance penalties	• Mixed results about effectiveness of monetary policies • Human error data breaches continue to flood the sector • Policy sometimes work on protecting data	Regression Variables • Patient records compromised • Monetary penalties paid • Human error data breach incidents

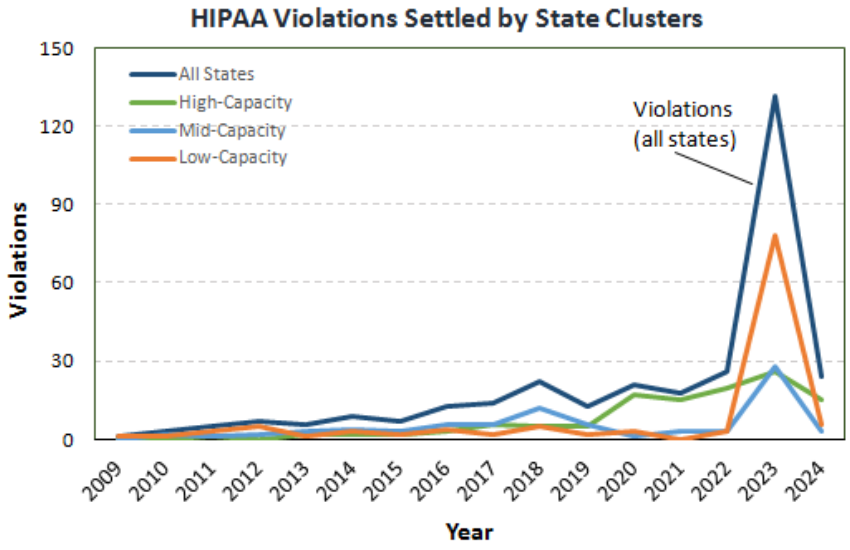
Table 31: Essay 2 Results from Semi-Structured Interviews and How the findings Inform th Research Study

Quantitative Data Results

Figures 19 and 20 illustrate that since 2009 a total of 321 violations have resulted in $380 million in penalty settlements across all DMUs. Notably, fiscal year 2023 accounted for 41% of all recorded violations and 29% of the total monetary penalties settled since 2009. The highest average number of violations and monetary settlements has been reported in the high-capacity states, highly populated states such as California, New York, and Texas, where a greater volume of patient records is at risk. Violations and penalties varies across the three state clusters with the highest penalties reported in high-capacity states.

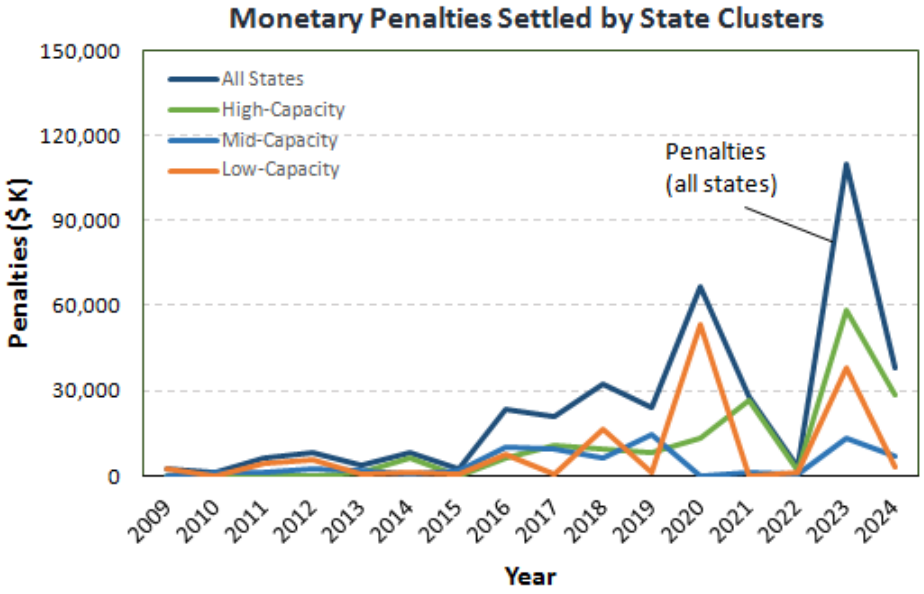
However, an exception to this trend is the $48.2 million settlement paid by Anthem Inc. in 2020, a company based in Indianapolis, Indiana which fall within the low-capacity states cluster. This settlement resulted from a multi-state investigation by state attorneys general over its 2014 data breach, which compromised 78.8 million patient records. Excluding this outlier, the trend in violations for the high-capacity and mid-

capacity states is consistent with the monetary penalty settlements number within these clusters.



Violations (Units)	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Avg Violations (All)	0.0	0.1	0.1	0.1	0.1	0.2	0.1	0.3	0.3	0.4	0.3	0.4	0.4	0.5	2.6	0.5
Avg Violation (High-Capacity)	0.0	0.0	0.3	0.0	0.7	0.7	0.7	1.0	2.0	1.7	1.7	5.7	5.0	6.7	8.7	5.0
Avg Violation (Mid-Capacity)	0.0	0.2	0.1	0.2	0.3	0.4	0.3	0.5	0.5	1.1	0.5	0.1	0.3	0.3	2.5	0.3
Avg Violation (Low-Capacity)	0.0	0.0	0.1	0.1	0.0	0.1	0.1	0.1	0.1	0.1	0.1	0.1	0.0	0.1	2.1	0.2

Figure 19: HIPAA Violations Settlements by State Clusters (2009-2024) (HIPAA, 2024)



Penalties ($ in Ks)	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Avg Penalty (All)	44	25	124	159	76	161	55	461	408	633	473	1,309	551	67	2,159	747
Avg Penalty (High-Capacity)	0	0	289	0	497	2,175	47	2,042	3,539	3,091	2,848	4,429	8,994	525	19,544	9,462
Avg Penalty (Mid-Capacity)	0	94	91	205	181	46	165	907	864	590	1,324	6	101	68	1,227	614
Avg Penalty (Low-Capacity)	61	7	120	158	11	32	23	200	18	446	27	1,443	0	29	1,027	79

Figure 20: HIPAA Penalty Payment Settlements by State Clusters (2009-2024) (HIPAA, 2024)

Results from the regression analysis indicate a statistically significant relationship in high-capacity states, where one-year lagged monetary penalties are strongly correlated with compromised patient records ($p < 0.05$). However, no significant relationship was found for mid-capacity and low-capacity states ($p > 0.05$). In these cases, the regression analysis did not support the hypothesis, and the null hypothesis (H_0) for both cases cannot be rejected. Additional details are provided in Table 32.

The findings indicate that the effectiveness of HIPAA monetary penalties in reducing compromised patient records varies by state capacity level. In high-capacity states, monetary penalties appear to have a stronger impact than in mid-capacity and low-capacity states reducing data breaches in these states. This aligns with insights from SMEs in the semi-structured interviews, where it was noted that high-capacity and mid-capacity states often prefer to pay the penalties rather than invest significantly in improving their IT infrastructure. While they adhere to monetary penalties, these fines alone do not serve as a sufficient deterrence for these healthcare systems. The statistical results from the multiple regression models testing this hypothesis across the high-capacity, mid-capacity, and low-capacity state clusters are presented in Appendix D.

Regression Test Results

High-Capacity States (IV)	N	R-Square	Estimate	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	44		0.1421	0.0663	4.02E+13		4.5846	2.14	0.0381
Patient Records (t-1)	44		0.5223	0.1844	7.03E+13		8.0235	2.83	0.0071
		0.4080				42			

Regression Test Results

Mid-Capacity States (IV)	N	R-Square	Estimate	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	164		-0.1236	0.1579	3.51E+12		0.6126	-0.78	0.4350
Patient Records (t-1)	164		0.1608	0.0779	2.44E+13		4.2639	2.06	0.04052
		0.0275				162			

Regression Test Results

Low-Capacity States (IV)	N	R-Square	Estimate	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	552		0.0712	0.1108	1.35E+13		0.4128	0.64	0.5208
Patient Records (t-1)	552		0.0555	0.0646	2.42E+13		0.7396	0.86	0.3902
		0.0021				550			

Table 32: Hypothesis 3 Testing Results for State Clusters with One-Year Lagged Independent Variables Using Compromised Patient Record at Time t as the Dependent Variable

In 2024 DHHS OCR implemented some adjustments to the HIPAA monetary penalties, primarily to account for annual inflation adjustments. However, no significant policy changes were introduced. These updates result in only a marginal increase in the financial penalties for non-compliant organizations, with very limited deterrence added against future violations.

4.6 Limitation

A limitation of using the HIPAA monetary penalty list to test the hypothesis for this essay is that the DHHS OCR dataset only includes settled violation fines. Not all HIPAA violations involving data breaches and compromised patient records result in monetary penalties. Many are resolved through technical assistance or corrective action plans instead. For example, in 2022, despite receiving over 300,000 complaints and reports of data breaches, the DHHS OCR issued fines or agreed settlements in only 110 cases (HIPAA, 2024). The majority of other cases, even where HIPAA violations were identified, were addressed through non-monetary resolutions.

Since not all breaches result in penalties, this limitation may introduce bias into the dataset, potentially affecting the statistical significance of the hypothesis testing. Additionally, in isolated cases it is noted that few violations are settled years after the initial non-compliance was reported. For instance, Anthem Inc., a health insurance provider based in Indianapolis, IN, settled a multi-state investigation by state attorneys general in 2020 for a data breach involving 78.8 million records that occurred in 2014.

4.7 Conclusion, Future Work, and Recommendation

The data trend and findings in this chapter demonstrate that monetary penalties from HIPAA violations have not been effective in slowing down the number of compromised patient records in the healthcare sector. Insights from interviews with SMEs suggest that HIPAA penalties are not severe enough to drive changes in the security of patient records. Organizations are failing to make necessary improvements despite facing financial consequences. In some cases, the penalties are so insignificant, relative to the cost of system improvements, that organizations find it more practical to simply pay the fines rather than invest in long-term cybersecurity enhancements.

An enhanced Reason's Resiliency Model (Figure 18) was utilized to assess the "Government Regulation" STS factor as a safeguard layer against patient record breaches resulting from human-technology interface errors. Multiple regression models were applied to analyze the relationship between HIPAA violation monetary penalties and the number of compromised patient records. The regression results indicate a strong statistical relationship between monetary penalties and compromised patient records in high-capacity states, where as a weak relationship for mid-capacity and low-capacity states.

The findings suggest that the effectiveness of HIPAA monetary penalties in reducing compromised patient records varies by state capacity level. In high-capacity states, the strong statistical relationship indicates that penalties may act as a stronger deterrent or drive more significant compliance efforts in these larger states. However, in mid-capacity and low-capacity states, the weak relationship suggests that increasing penalties alone may not be sufficient to reduce data breaches in these states.

These findings indicate that a HIPAA policy change to increase the monetary penalties to prevent data breaches would not necessarily result in a nationwide reduction to the number of compromised patient records. Further research is needed to assess whether security measures implemented by organizations improve in the years following a penalty, could provide more insights into the long term effectiveness of HIPAA monetary penalties. Additionally, a proposal should be submitted to DHHS OCR with proposed measures to strengthen enforcement and mitigation efforts, that would enhance accountability, improve compliance, and better protect patient data from future breaches.

A notable disconnect exists between the statistical findings in Essay 3 and the perspectives of subject matter experts (SMEs) regarding the impact of HIPAA monetary penalties on reducing compromised healthcare records in high-capacity states. While SMEs generally argue that these penalties have limited deterrent effect, pointing out that the fines are often not severe enough to compel action, and that high-capacity

states may opt to pay the penalties rather than invest in addressing IT vulnerabilities, the hypothesis tested in Essay 3 revealed a statistically significant association between higher penalties and a reduction in compromised records. This contrast highlights the importance of conducting more capacity-sensitive analyses when evaluating the effectiveness of regulatory interventions for different states groups.

Recommendation

To strengthen HIPAA violation mitigation efforts, penalties should be made more severe. Along with stricter monetary penalties, a proposal should be submitted to the DHHS OCR, outlining the following recommendations to enhance HIPAA compliance and minimize the risk of data breaches resulting from human error:

- Implement Minimum Information Security Rating System: Require healthcare organizations to maintain a minimum security rating to continue operations. Entities falling below a certain threshold should face restrictions on their ability to conduct business and provide services.
- Mandate Patient Compensation Funds: Establish a fund, fully financed by the violating entity, to provide financial support and identity protection services to affected individuals.
- Mandate Public Disclosure of Violations: Mandate transparency in violation investigations and the corrective measures taken to enhance information security.
- Enforce a Tiered Penalty Structure: Implement escalating penalties for repeat violations, including operational restrictions and service suspensions until compliance improvements are made.

Insights from SMEs gathered through semi-structured interviews, along with findings from the literature review, inform these recommendations aimed at strengthening state healthcare systems by implementing a more structured and disciplined program to ensure compliance with government regulations, such as HIPAA and other IT security policies.

4.8 References

[1] Alder, S., (2021). Future of HIPAA: Reflections at the 25th Anniversary of HIPAA. HIPAA Journal.

[2] American University-Public Policy Department, (2023). The Evolution of Public Policy. American University Publication.

[3] Belanger, F., Crossler, R.E., (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly.

[4] Borras, S., Edler, J., (2020). The Roles of the State in the Governance of Socio-Technical Systems Transformation. Elsevier.

[5] DeCamp, W., Herskovitz, K., (2015). The Theories of Accident Causation. Research Gate.

[6] Department of Health and Human Services - Office for Civil Rights, (2023). HIPAA Compliance Checklist. Health Information Privacy.

[7] Department of Health and Human Services - Office for Civil Rights, (2022). Summary of the HIPAA Privacy Rule. Health Information Privacy.

[8] Department of Health and Human Services - Office for Civil Rights, (2022). Summary of the HIPAA Security Rule. Health Information Privacy.

[9] Goldberg, A.T., (2003). Incident Investigation: Rethinking the Chain of Events Analogy. EHS Today.

[10] Health Insurance Portability and Accountability Act, (2022). Healthcare Data Breach Statistics. Department of Health and Human Services.

[11] Health Insurance Portability and Accountability Act (HIPAA), (2024). HIPAA History. Department of Health and Human Services- The HIPAA Journal.

[12] Heinrich, H. W., Petersen, D., Roos, N., (1980). Industrial Accident Prevention. New York: McGraw-Hill.

[13] Horne, C.A., Ahmad, A., Maynard, S.B., (2016). A Theory of Information Security. Australasian Conference on Information Systems.

[14] Jensen, R.A., (2022). U.S. Investments in Medical and Health Research and Development. Research America.

[15] Johnson, L., (2022). How Long Does a HIPAA Investigation Take? The HIPAA Guide.

[16] Leveson, N.G., (2004). A New Accident Model for Engineering Safer Systems. Reading. MA: Addison Wesley.

[17] Leveson, N.G., Daouk, M., Dulac, N., Marais, K., (2003). Applying STAMP in Accident Analysis. Semantic Scholar.

[18] Mathews, K., (2018). HIPAA Compliance and the HITECH Act in 2018. Health IT.

[19] McCumber, J., (1991). Information Systems Security: A Comprehensive Model. Proceedings of the 14th National Computer Security Conference, Washington: National Institute of Standards and Technology. National Computer Security Center.

[20] Pawar, P., Jones, V., Van Beijnum, B.J.F., Hermens, H., (2012). A Framework for the Comparison of Mobile Patient Monitoring Systems. Journal of Biomedical Informatics.

[21] Perneger, T.V., (2005). The Swiss Cheese Model of Safety Incidents: Are There Holes in the Metaphor? BMC Health Services Research.

[22] Posthumus, S., Von Solms, R., (2004). A Framework for the Governance of Information Security. Computers & Security (23:8), pp 638-646.

[23] Qureshi, Z.H., (2008). A Review of Accident Modelling Approaches for Complex Critical Socio-Technical Systems. Defense Science and Technology Organization.

[24] Reason, J., (2000). Human Error: Models and Management. British Medical Journal (BMJ).

[25] Reason, J., Hollnagel, E., Paries, J., (2006). Revisiting the Swiss Cheese Model of Accidents. Eurocontrol Experimental Centre.

[26] Schwarats, B., (2021). The Swiss Cheese Model: Designing to Reduce Catastrophic Losses.

[27] Smith, A., Stirling, A., Berkhout, F., (2005). The Governance of Sustainable Socio-Technical Transitions. Elsevier.

[28] Theodos, K., Sittig, S., (2020). Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply. National Library of Medicine.

[29] Von Solms, R., (1998). Information Security Management (3): The Code of Practice for Information Security Management (Bs 7799). Information Management & Computer Security (6:5), pp 224-225.

Appendix D

Regression Results for Essay 3 Hypothesis. The Table Presents Results for Multiple Models for Each State Cluster Using Compromised Patient Records as the Dependent Variable.

High-Capacity States

Model 1 Regression Test Results

High-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F Ratio	T-Ratio	P-Value
Monetary Penalties	47	0.2968	0.0564	1.91E+14	46	19.418	0.06	<0.0001

Model 2 Regression Test Results

High-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F Ratio	T-Ratio	P-Value
Data Breaches	47	0.4912	17,462	3.15E+14	46	44.4155	6.66	<0.0001

Model 3 Regression Test Results

High-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties	47		0.0530	3.29E+13		5.037	2.94	0.0298
Data Breaches	47		19,297	1.58E+14		24.1572	4.91	<0.0001
		0.5424			45			

Model 4 Regression Test Results

High-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	44	0.2949	0.0588	1.83E+14	43	17.9883	4.24	0.0001

Model 5 Regression Test Results

High-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	44		0.0663	4.02E+13		4.5846	2.14	0.0381
Patient Records (t-1)	44		0.1844	7.03E+13		8.0235	2.83	0.0071
		0.4080			42			

Model 6 Regression Test Results

High-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	44		0.0567	2.27E+13		3.6191	1.90	0.0642
Patient Records (t-1)	44		0.1687	1.40E+13		2.2358	1.50	0.1425
Data Breaches	44		20,336	1.11E+14		17.6936	4.21	0.0001
		0.5865			41			

Model 7 Regression Test Results

High-Capacity States (IV)	N	R-Square	Std. Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	41		0.0614	2.11E+13		3.0474	1.75	0.0892
Patient Records (t-1)	41		0.1783	1.41E+13		2.0356	1.43	0.1620
Monetary Penalties (t-2)	41		0.1149	1.60E+08		0.0000	0.00	0.9962
Data Breaches	41		24,161	9.03E+13		13.0343	3.61	0.0009
		0.5715			37			

Model 8 Regression Test Results

High-Capacity States (IV)	N	R-Square	Std. Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	41		0.0599	2.57E+13		3.7942	1.95	0.0590
Patient Records (t-1)	41		0.1798	1.00E+13		1.4767	1.22	0.2320
Patient Records (t-2)	41		0.2004	5.71E+12		0.8421	0.92	0.3647
Data Breaches	41		23,790	7.43E+13		10.9604	3.31	0.0021
		0.5810			37			

Model 9 Regression Test Results

High-Capacity States (IV)	N	R-Square	Std Eror	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-2)	41		0.1224	1.65E+12		0.1986	-0.45	0.6584
Patient Records (t-2)	41		0.2162	6.59E+12		0.7913	0.89	0.3793
Data Breaches	41		25,427	1.70E+14		20.3578	4.51	<0.0001
		0.4711			38			

Mid-Capacity States

Model 1 Regression Test Results

Mid-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties	175	0.0078	1,095,509	7.5971E+12	174	1.3762	1.17	0.2423

Model 2 Regression Test Results

Mid-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Data Breaches	175	0.2031	1,095,509	1.9663E+14	174	44.35	6.66	<0.0001

Model 3 Regression Test Results

Mid-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties	175		0.1320	1.65E+12		0.3709	0.61	0.5431
Data Breaches	175		15,230	1.91E+12		42.8515	6.55	<0.0001
		0.2048			173			

Model 4 Regression Test Results

Mid-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	164	0.0019	0.1586	1.84E+12	163	0.3143	-0.56	0.5758

Model 5 Regression Test Results

Mid-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	164		0.1579	3.51E+12		0.6126	-0.78	0.4350
Patient Records (t-1)	164		0.0779	2.44E+13		4.2639	2.06	0.04052
		0.0275			162			

Model 6 Regression Test Results

Mid-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	164		0.1440	6.16E+12		1.2971	-1.14	0.2564
Patient Records (t-1)	164		0.0776	4.61E+11		0.0972	-0.31	0.7556
Data Breaches	164		17,925	1.63E+14		34.384	5.86	<0.0001
		0.1987			161			

Model 7 Regression Test Results

Mid-Capacity States (IV)	N	R-Square	Std. Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	153		0.1499	6.17E+12		1.2023	-1.1	0.27463
Patient Records (t-1)	153		0.0809	4.75E+11		0.0926	0.3	0.7613
Monetary Penalties (t-2)	153		0.1525	2.53E+10		0.002	-0.07	0.9441
Data Breaches	153		19,335	1.51E+14		29.436	5.43	<0.0001
		0.1866			149			

Model 8 Regression Test Results

Mid-Capacity States (IV)	N	R-Square	Std. Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	153		0.1473	5.64E+12		1.1398	-1.07	0.2874
Patient Records (t-1)	153		0.0798	1.72E+12		0.3472	-0.59	0.5566
Patient Records (t-2)	153		0.1061	2.70E+13		5.4540	2.34	0.0209
Data Breaches	153		19,479	1.15E+14		23.2192	4.82	<0.0001
		0.2153			149			

Model 9 Regression Test Results

Mid-Capacity States (IV)	N	R-Square	Std Eror	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-2)	153		0.1496	2.03E+09		0.0004	-0.02	0.9839
Patient Records (t-2)	153		0.1055	2.60E+13		5.2366	2.29	0.0235
Data Breaches	153		18,288	1.16E+14		23.4355	4.84	<0.0001
		0.2069			150			

Low-Capacity States

Model 1 Regression Test Results

Low-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties	590	0.0008	0.0727	6.73E+12	589	0.4767	0.69	0.4902

Model 2 Regression Test Results

Low-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Data Breaches	590	0.0338	49,896	6.10E+14	589	20.6226	4.54	<0.0001

Model 3 Regression Test Results

Low-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties	590		0.1065	2.85E+12		0.0838	-0.29	0.7723
Data Breaches	590		50,480	6.09E+14		20.5314	4.53	<0.0001
		0.0339			588			

Model 4 Regression Test Results

Low-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	552	0.0008	0.1106	1.46E+13	552	0.4476	0.67	0.5037

Model 5 Regression Test Results

Low-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	552		0.1108	1.35E+13		0.4128	0.64	0.5208
Patient Records (t-1)	552		0.0646	2.42E+13		0.7396	0.86	0.3902
		0.0021			550			

Model 6 Regression Test Results

Low-Capacity States (IV)	N	R-Square	Std Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	552		0.1104	2.98E+09		0.0001	0.01	0.9923
Patient Records (t-1)	552		0.0646	4.76E+11		0.0150	0.12	0.9026
Data Breaches	552		54,353	5.55E+14		17.4721	4.18	<0.0001
		0.0329			549			

Model 7 Regression Test Results

Low-Capacity States (IV)	N	R-Square	Std. Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	515		0.1145	1.04E+09		0.0000	0.01	0.9956
Patient Records (t-1)	515		0.0670	4.58E+11		0.0134	0.12	0.9079
Monetary Penalties (t-2)	515		0.1149	3.10E+11		0.0091	-0.10	0.9241
Data Breaches	515		58,136	5.31E+14		15.5569	3.94	<0.0001
		0.0319			511			

Model 8 Regression Test Results

Low-Capacity States (IV)	N	R-Square	Std. Error	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-1)	515		0.1147	7.01E+07		0.0000	0.00	0.9989
Patient Records (t-1)	515		0.0670	4.19E+11		0.0123	0.11	0.9119
Patient Records (t-2)	515		0.0697	6.39E+12		0.1871	-0.43	0.6655
Data Breaches	515		57,864	5.45E+14		15.9635	4.00	<0.0001
		0.0323			511			

Model 9 Regression Test Results

Low-Capacity States (IV)	N	R-Square	Std Eror	Sum of Square	DF	F-Ratio	T-Ratio	P-Value
Monetary Penalties (t-2)	515		0.1147	3.08E+11		0.0090	-0.10	0.9243
Patient Records (t-2)	515		0.0695	6.41E+12		0.1883	-0.43	0.6645
Data Breaches	515		56,785	5.74E+14		16.8530	4.11	<0.0001
		0.0323			512			

Chapter 5.0: Conclusion, Future Work, Limitation, and Recommendation

Conclusion and Future Work

This dissertation concludes that addressing EHR information security threats requires a fundamental shift in the healthcare sector's approach to data security. The research determines that integrating technological, organizational, human, and government regulatory STS factors into Reason's layered approach offers a comprehensive management framework for mitigating human error challenges in healthcare information security. The framework builds on Reason's Resiliency Model by incorporating a socially oriented management approach based on socio-technical system (STS) principles. The framework is designed to mitigate human error in information security, aiming to enhance the resilience of EHR systems against data breaches and make them less attractive to cybercriminals.

This dissertation examines the impact of human error on information security in the healthcare sector, as a consequence of the human-technology interface. A systematic literature review was conducted, analyzing 1,071 documents to inform the research. From this review, two conceptual frameworks were developed: a taxonomy categorizing human errors leading to data breaches, and a management framework based on STS principles. The findings identified a gap in terms of understanding and modeling of human-computer interactions, as well as the need for greater consideration of STS factors when designing information security solutions.

Comprehensive datasets of current healthcare IT systems support the modeling and hypothesis testing designed to address the research questions across the three essays. Empirical analysis, benchmarking assessments, and regression models derived from these datasets provide key insights into the role of human error in patient record security, the productivity performance of state healthcare systems (DMUs), and the influence of HIPAA policy on the volume of compromised records in the sector.

Clustering algorithms were applied to account for differences in the characteristics of the DMUs, which contribute to variability in the data. Principal component analysis (PCA) was used to reduce the dataset's dimensionality and DBSCAN clustering algorithms to identify the optimal number of clusters (Greenacre et al., 2023). A K-Means clustering algorithm was then applied using gross domestic product (GDP) and population as the primary factors for grouping states into distinct and non-overlapping clusters (Yadav et al., 2013). As a result, DMUs were categorized into three clusters: high-capacity states, mid-capacity states, and low-capacity states. These clusters represent each state's ability to provide healthcare services relative to demand.

An empirical analysis of all healthcare cybersecurity incidents reported since 2009 reveals that the location where data are breached influences the severity of data breaches impacting patient information privacy. The analysis shows that network servers and emails are the two most common sites where healthcare data are breached capturing 95% of the 713 million patients' records compromised since 2009. These findings have real-world implications for the security of healthcare data. It enables the development of more effective incident response and containment processes to shorten the data exposure at network servers and email traffic. It also supports healthcare resources decisions to address IT system vulnerabilities aiming at reducing recurring human-technology interface errors that could result in patient record data breaches.

Semi-structured interviews were conducted with subject matter experts (SMEs) to get insights from cybersecurity and healthcare professionals on the nuances in information security and patient care services that were not evident in the literature. The findings from the interviews confirm that data transfer and password hygiene are the most common human error. Consequently, these errors drive emails and access to network servers as the most common locations where data are breached. SMEs agree that breaches create a disruption in patient care services, data protection concerns when sharing patient's information with industry peers, and result in an overall cost increase for healthcare organizations. Most SMEs believe that HIPAA penalties are not severe

enough, and that for middle and large size healthcare organizations writing a penalty check is more economically feasible than correcting vulnerabilities in their IT systems.

The Malmquist Performance Index (MPI) was used for analyzing and comparing the productivity changes and efficiency improvements of state healthcare systems (DMUs) (Mostoli et al., 2019). Results from the MPI model show that, despite declines in productivity among high-capacity and mid-capacity states, significant gains in low-capacity states have more than compensated for these losses, resulting in an overall increase in healthcare sector productivity over time. These results highlight the critical role of digital platforms adoption in enhancing healthcare productivity performance, despite unintended consequences such as privacy concerns. However, cybersecurity threats continue to impact the productivity of the DMUs. Notably, low-capacity states have effectively balanced EHR technology advancements with privacy safeguards, leading to improved patient care services over time.

The ANOVA test was used to determine if the differences of the MPI results from the three state clusters were statistically significant. While EHR adoption has contributed to overall productivity gains, the one-way ANOVA test results did not confirm significant differences exist in MPI among the high-capacity, middle-income, and low-capacity state clusters, suggesting that the impact of EHR adoption on productivity, despite increasing privacy concerns, is not statistically significant across the groups. Furthermore, regression analysis findings revealed a weak relationship between compromised patient records and monetary penalties predictors, and the MPI across all state categories.

The data analyzed in Chapter 4 confirm that monetary penalties from HIPAA policy violations have not been effective in slowing down the number of compromised patient records. Results from the regression analysis performed to test the hypothesis, that monetary penalties are positively correlated with a reduction in the number of compromised patient records, indicate a strong relationship between one-year lagged monetary penalties and compromised patient records in high-capacity states, whereas

this relationship is not significant for mid-capacity and low-capacity states. In high-capacity states, the strong statistical relationship indicates that penalties may serve as a stronger deterrent or drive more compliance efforts. However, investments in their IT security systems seem insufficient, as they continue to face vulnerabilities that cyber attackers continue to exploit. In some cases, penalties are so insignificant that these organizations find it more cost-effective to pay the fines rather than commit to long-term cybersecurity enhancements.

In mid-capacity and low-capacity states, the weak relationship suggests that simply increasing penalties may not be enough to reduce data breaches. The findings indicate that current penalties are not severe enough to serve as an effective deterrent. Financial penalties alone fail to sufficiently discourage healthcare providers from repeated data breaches, leading to sustaining risks to patients' sensitive health information.

A notable disconnect exists between the statistical findings in Essay 3 and the perspectives of subject matter experts (SMEs) regarding the impact of HIPAA monetary penalties on reducing compromised healthcare records in high-capacity states. While SMEs generally argue that these penalties have limited deterrent effect, pointing out that the fines are often not severe enough to compel action, and that high-capacity states may opt to pay the penalties rather than invest in addressing IT vulnerabilities, the hypothesis tested in Essay 3 revealed a statistically significant association between higher penalties and a reduction in compromised records. This contrast highlights the importance of conducting more capacity-sensitive analyses when evaluating the effectiveness of regulatory interventions for different states groups.

The enhanced Reason's Resiliency Model presented in Chapter 2 represents a culture shift from the way that the sector has been approaching data security, from purely technical design solutions to dynamic socio-technical solutions. Chapter 4 applied the model to the Government Regulation STS factor to test the effectiveness of HIPAA monetary policy influencing the number of compromised patient records in the sector.

- Future Work - Open Research Problem: “Assess the impact of other socio-technical system factors to include technological, organizational, and human in the loop factors, influencing the number of compromised patient records.”

  Further research is recommended to investigate additional socio-technical system (STS) factors beyond Government Regulations that affect information security concerns related to data breaches. Investigating other STS factors, such as human error, organizational policies, and technological advancements, is crucial for providing a comprehensive assessment of how these factors influence the number of compromised patient records. This issue remains unresolved and represents a critical area for research aimed at understanding how various components of STS interact to address the challenge of compromised patient records. Understanding the results of these interactions is essential for developing effective strategies to enhance patient safety and data security within healthcare systems.

The MPI results from Chapter 3 indicate the productivity performance of healthcare providers in low-capacity states has increased, while high-capacity and mid-capacity state clusters have experienced a decline over time.

- Future Work - Open Research Problem: “Explore the impact of socio-economic and demographic variables in the productivity performance of state healthcare systems.”

  Further research is recommended to explore how socio-economic, government policy such as HIPAA and demographic variables, like age distribution, education level, and population density, affect the productivity of healthcare providers across different state clusters. Given the dataset’s high-dimensionality, potentially containing thousands of observations across various demographic factors, advanced analytical tools, such as artificial intelligence models, may be required for efficiently processing the data and conducting the linear programming modeling needed for the benchmarking analysis.

- Future Work - Open Research Problem: “Study the impact of data breaches on healthcare outcomes. Specifically, conduct an analysis of the relationship between compromised patient records and mortality rates.”

  The increasing frequency of data breaches in healthcare systems raises critical concerns about patient safety and care quality. When patient records are compromised, there is a risk of erroneous information being introduced into EHR. Such erroneous information can lead to incorrect diagnoses, inappropriate treatments, and ultimately, increased mortality rates. Furthermore, the aftermath of data breaches often necessitates the implementation of additional security measures and system fixes, which can disrupt clinical workflows and divert resources away from patient care. The literature highlights that healthcare organizations reported increased mortality rates after significant data breaches, due to delays in procedures and tests. For instance, a study from Vanderbilt University, “Data Breach Fixes Could Impact Patient Care: Study,” highlights that following a data breach, hospitals experienced delays in administering electrocardiograms and observed a rise in 30-day mortality rates for heart attack on patients, with up to 36 additional deaths per 10,000 heart attacks annually (Vanderbilt University, 2019).

  These findings stress the need for research to analyze the correlation between data breaches and mortality rates, aiming to understand the seriousness of this relationship and develop strategies to protect patient information.

- Future Work - Open Research Problem: “Explore the impact of modeling the Managed Patients input variable as an environmental variable in the Malmquist Productivity Index (MPI).”

  Future studies should also explore the impact of modeling Managed Patients as an environmental variable in the MPI when assessing the productivity of state healthcare systems. Since patient volume is largely determined by external factors such as population size and public health demands, which are conditions

beyond the control of individual systems, treating it as an input variable may impact efficiency scores and unfairly disadvantage high-capacity state healthcare systems. Incorporating Managed Patients as a non-discretionary, environmental factor can lead to more accurate benchmarking by adjusting for contextual differences and better isolating true operational inefficiencies.

The findings from Chapter 4 help assess the effectiveness of HIPAA monetary penalties, addressing their limited deterrence effect as they fail to discourage DMUs from repeatedly compromising patient records.

- Future Work- Open Research Problem: "Assess limitations of HIPAA monetary penalties as a deterrent of data breach incidents."

  Further research should focus on evaluating the limitations of HIPAA monetary penalties as deterrents to data breaches in the healthcare sector. The current dataset, which focuses on HIPAA violations resulting in monetary penalties, may have introduced bias by excluding violation instances addressed through technical assistance or corrective action plans without financial penalties. This dataset limitation may have potentially affected the statistical significance of the tested hypothesis. Therefore, assessing limitations of HIPAA monetary penalties, is still an open research problem that needs to be studied to fully determine the effectiveness of Government Regulation influencing the number of compromised patient records.

  This open research area should encompass all forms of penalties and their resolutions, including monetary penalties, technical assistance, and corrective action plans. The result of this analysis could provide a clearer understanding of the effectiveness of HIPAA enforcement in reducing breaches of protected health information. A thorough assessment of these enforcement strategies is essential to develop more effective policies for safeguarding patient health information.

The landscape of human privacy is changing and becoming more challenging as we move more and more of our lives into the digital space. Although most of our lives are now stored somewhere online, the healthcare sector must realize the risks involved in the ways in which protected health data is being used once records are stored digitally. Hopefully the implementation of long term resilience capabilities with greater attention to STS factors in the design of information security solutions will lead to a change, and better protection of patient information privacy (Alvarado, Triantis, 2024).

Limitation

This dissertation faced several challenges, including limitations in the literature, difficulties in data collection, and constraints in data availability, which impacted the analysis.

One key challenge in this research was the limited body of literature specifically addressing the human aspect of data breaches and cybersecurity within healthcare. Most existing studies were conducted in the United States, with little attention from the international research community on how human error data breaches impact EHR adoption and information sharing. While this gap in the literature presented an opportunity to explore an innovative solution, the absence of relevant studies posed challenges by limiting the foundational knowledge available for this study.

Semi-structured interviews with SMEs were introduced to compensate for the limited amount of data in the literature related to the application of STS principles to solve human error challenges in IT. These interviews provided valuable insights, enhanced knowledge depth, and strengthened the dissertation's foundation.

However, coordinating the interview sessions was challenging, leading to fewer sessions than initially planned. In most cases, SMEs would not necessarily volunteer time to provide their views for a session unless the interviewer had an existing relationship, or a prior connection with the SME through other means. Additionally, the post interview process required extensive analysis of interview notes, often requiring

follow-ups with SMEs to ensure accurate interpretation and synthesis of their views and perspectives into a usable and meaningful product to inform the dissertation.

A limitation of using the HIPAA monetary penalty list to test the hypothesis on policy effectiveness as a deterrent to data breach incidents is that the DHHS OCR dataset only includes settled violation fines. A very small percentage of HIPAA violations involving data breaches and compromised patient records result in monetary penalties, as most are resolved through technical assistance or corrective action plans. This limitation may have introduced bias into the dataset, potentially impacting the statistical significance of the hypothesis testing.

Recommendation

Findings from the literature in Chapter 2 highlight that robust technical design solutions and government policy play an important role in information security, but they are not sufficient to mitigate data breaches of EHR. An alternative approach is needed, to bridge this gap DMUs should:

- Adopt the Enhanced Reason's Resiliency Model (Figure 3): The proposed model follows a layered design approach, incorporating STS factors identified in the literature as effective in reducing human error-related data breaches. It represents a cultural shift from the sector's current reliance on purely technical design solutions and toward a socio-technical design environment, where technological, organizational, human, and government factors are integrated to improve EHR information security.

Results from Chapter 2 also identified the most vulnerable locations within healthcare IT systems where data breaches frequently occur due to human-technology interface errors. To enhance IT systems security, the following proactive measures are recommended for the state healthcare systems (DMUs):

- Predefined Incident Response and Containment Strategies: Develop a comprehensive library of security patches that can be ready available to implement when a data breach incident is identified. This approach helps

minimize data exposure time, accelerate patient care service restoration, and reduce overall breach-related costs.

- Routine Penetration Testing and Security Audits: Develop a structured plan to routinely test known system vulnerabilities, such as network servers and emails, and implement security enhancements. Regular assessments and testing will help prevent recurring data breaches and ensure continuous improvement in the IT system security.

To mitigate the impact of unintended consequences, such as information privacy concerns resulting from technology adoption, healthcare organizations should implement proactive measures. The following recommendations can help reduce the impact of data breach incidents and improve the productivity of state healthcare systems (DMUs):

- Implement Annual Information Security Audits: Healthcare organizations should adopt regular security audits, similar to financial audits for large corporations, to ensure their systems effectively protect patient health information and prevent recurring breaches.
- Acquire Information Protection Malpractice Insurance: Healthcare entities must carry an information security malpractice insurance, specifically covering incidents where patient privacy is compromised due to human-error negligence, or system security failures.

To strengthen HIPAA violation mitigation efforts, penalties should be made more severe. Along with stricter monetary penalties, a proposal should be submitted to the Department of Health and Human Services- Office of Civil Rights (DHHS-OCR), outlining the following recommendations to enhance HIPAA compliance and minimize the risk of data breaches resulting from human error:

- Implement Minimum Information Security Rating System: Require healthcare organizations to maintain a minimum security rating to continue operations. Entities falling below a certain threshold should face restrictions on their ability to conduct business and provide services.

- Mandate Patient Compensation Funds: Establish a fund, fully financed by the violating entity, to provide financial support and identity protection services to affected individuals.
- Mandate Public Disclosure of Violations: Mandate transparency in violation investigations and the corrective measures taken to enhance information security.
- Enforce a Tiered Penalty Structure: Implement escalating penalties for repeat violations, including operational restrictions and service suspensions until compliance improvements are made.

Implementing these recommendations expeditiously and concurrently will be a significant challenge. Achieving meaningful progress will require strong commitment and leadership from both Congressional and Executive Branch Officials, as well as the proactive engagement from state healthcare systems (DMUs) management. Their collective efforts will be essential in achieving sustainable improvements in patient information security while enhancing the overall quality of healthcare services. Leadership from DHHS OCR and DMUs must play a critical role driving collaboration, sharing lessons learned, and embracing a unified approach to build the desired future-state: a highly productive and secure healthcare system for the American people.

Appendix E
Glossary

Analysis of Variance (ANOVA): A statistical test used to analyze the difference between the means of more than two groups.

Business Associates: Third party administrators that provide services such as accounting and legal support to healthcare providers.

Cybersecurity: Practice of protecting critical systems and sensitive information from digital attacks.

Data Envelopment Analysis (DEA): A mathematical method using linear programming techniques to convert inputs to outputs with the purpose of evaluating the performance of comparable organizations or products.

Decision Making Units (DMUs): A group of individuals or stakeholders involved in the process of making decisions related to purchasing goods or services.

Department of Health and Human Services (DHHS): U.S. Federal Government department whose mission is to enhance the health and well-being of all Americans, by providing for effective health and human services.

Electronic Health Records (EHR): Digitized version of a patient's health record paper charts.

Healthcare Clearing Houses: Organizations that translate claims from a nonstandard format into a standard transaction on behalf of a health care provider.

Healthcare Data Breaches: When an individual name plus a medical record are put at risk because of exposure through either electronic or paper means.

Health Information Technology for Economic and Clinical Health (HITECH) Act: Act enacted as part of the American Recovery and Reinvestment Act of 2009 that promotes the adoption and meaningful use of health information technology.

Health Insurance Portability and Accountability Act (HIPAA): The primary law that oversees the use and access to and disclosure of protected health information. It regulates how this data is created, collected, transmitted, maintained and stored by any HIPAA-covered organization.

Human Error: Any human action or lack thereof that leads to exceeding the tolerances of the conditions defined for the normative work of the analytical/measurement system with which the human interacts.

Identity Access Management (IAM): A system that implement technical security measures and procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Intentional Errors: Human errors where the employee understands the risk of his/her behavior but acts on it. It may not bring an immediate harm to the organization, but it may result in a data breach or a violation.

K-Means Clustering: A partitioning method that divides data into a predefined number (K) of clusters. The algorithm assigns each data point to the nearest cluster center, recalculates cluster centers iteratively, and minimizes the sum of squared distances between data points and the corresponding cluster center.

Malicious Errors: Human errors that are caused when the behavior of the employee is intentional and can have major damaging consequences. This is the worst type of error.

Malmquist Productivity Index (MPI): A measure that evaluates the productivity performance change of a decision-making unit over time. It is based on the concept of production function.

Protected Health Information (PHI): Health information data that relates to an individual; the payment for the provision of healthcare to an individual.

Socio-Technical Systems (STS): It is an approach to complex organizational work design that considers requirements from the interaction between people, technology, government policy, and organization aspects in workplaces.

Systems Theory: It is the interdisciplinary study of systems, i.e. cohesive groups of interrelated, interdependent parts that can be natural or human-made.

Unintentional Human Errors: Errors that can be due to the lack of knowledge or skills, or simply a distraction from the employee performing the tasks.

Zero Trust Principles: A security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

Appendix F

Semi-Structured Interview Protocols

Human Error in Electronic Health Records (EHR) Information Security

Semi-Structured Interview Questionnaire

Cybersecurity, Healthcare, and Policy Subject Matter Experts

Research Aim: Investigate the Impact of Human Technology Interface Error on EHR Information Security.

Research Interest: The purpose of this research is to study the impact of error, as a consequence of the human-technology interface, in the information security of the healthcare sector. The significance of the problem is undisputable, as the present day healthcare industry has become the main victim of external and internal cybersecurity incidents with some major publications reporting that over 80% of all data breaches are caused by an employee mistake, despite continuous investments in cybersecurity for addressing the problem. The literature demonstrates the value of adoption of EHR technology to improve healthcare quality of services, as well as strong evidence that information security ranks at the top of all challenges faced by the healthcare industry. The implementation of EHR technology demands protecting the privacy and security of patients' healthcare information, and the trends of data breaches resulting from human error suggest improvements in healthcare information systems (Alvarado, Triantis, 2024).

Purpose of Semi-Structured Interviews: Semi-structured interviews will enable collection of qualitative data to support this research study. The interviews aim to provide a better understanding of the role of human error in data breaches; unintended consequences of information technology adoption such as human error data breaches on the productivity performance of patient care services; and, perspective from stakeholders on the effectiveness of HIPAA policy reducing breaches in the sector. Information obtained from the semi-structured interviews will be used to validate results found in the literature.

The interview questions are designed to capture the following focus areas:

- Your experience with human-technology interface errors that have led to data breaches of protected personal information within your organization;
- How the compromise of protected personal information have affected the performance of your organization; and,
- How compliance with government policy influences your organization's management behavior towards improving information security systems.

Objective 1: Examine Human Technology Interface Error in Healthcare Organization's Data Breaches

Background: Human error data breaches refer to security incidents in which sensitive or confidential healthcare information is exposed, compromised, or mishandled due to mistakes made by humans interacting with technology. These errors can occur at various levels within the healthcare organization and may involve multiple actions such as accidentally emailing sensitive information to the wrong recipient, misconfiguring the identity access security settings, lack of awareness, failure to follow established security protocols, or improperly implementing government policy (Alvarado, Triantis, 2024). Highly technological systems, such as healthcare systems design to improve patient safety, are exceedingly becoming more complex. A primary characteristic of these systems is the high degree of human-technology collaboration required to deliver outcomes that couldn't be possible in isolation. An adverse consequence of the digitization of healthcare records has been the rapid ascent of cybersecurity incidents, primarily driven by human error and data breaches that are jeopardizing the privacy and security of patients' healthcare information (PHI). When electronic health records (EHR) are compromised, adoption of EHR and the patient safety and private information are put at risk (Alvarado, Triantis, 2024).

Questions:

1. Why should healthcare organizations care about cyber security and the risks of human errors that will result in data breaches?

2. What are some common situations where human errors led to security breaches in your healthcare organization?

3. What factors from the list below have the most impact in reducing the risk of human errors that result in healthcare data breaches?
   a) System identity access management (access credentials validation system)
   b) System diversity (common standard applications, simplicity of system)
   c) Business processes (user training, good written procedures, continuous management involvement, processes automation)
   d) Cyber security protocols (system security practices, system incident reports)
   e) Human in the loop (well defined external interfaces, effective design of Human-computer interfaces, employee competence level)
   f) User awareness (employee motivation, time pressure, stress/fatigue)
   g) Government policy (policy compliance, management oversight)

Objective 2: Unintended Consequences from Adoption of EHR Technology: Evaluating the Effect of Information Privacy Concerns from Human Error Data Breaches on Patient Care Services Performance.

Background: This objective investigates patients' information privacy concerns, as unintended consequences from the adoption of EHR technology, and their impact to patient care services. While the adoption of technology systems have resulted in substantial benefits to patient care, serious unintended consequences involving patients' information privacy have emerged during their implementation. For example, adoption of poor EHR system designs and improper use have resulted in EHR-human related errors that compromised private health information from millions of patient records. These unintended consequences have also put in danger patient safety, information privacy, and have decreased the quality of patient care services. Moreover, evidence found in the literature shows that these unintended consequences are also taking a toll on the productivity performance of healthcare providers as they have resulted in legal cases causing major disruptions in their operations, loss in trust and reputation in the organization's IT systems, and major financial losses.

Questions:

1. How patients' information privacy concerns have affected performance of patient care services within the healthcare organization?

2. How do healthcare professionals navigate privacy concerns when accessing and sharing patient information to coordinate care and collaborate with other members of the healthcare team?

3. How do patients' perceptions of privacy and confidentiality impact their willingness to disclose sensitive information or engage with healthcare services following a data breach or records have been compromised?

Objective 3: Application of HIPAA Policy as a Safeguard Layer to Reduce Human Error Data Breaches

Background: Health Insurance Portability and Accountability Act (HIPAA) is the primary law that oversees the use and access to and disclosure of patients protected health information (PHI). It regulates how this data is created, collected, transmitted, maintained and stored by any HIPAA-covered organization. The literature reports that HIPPA and subsequent amendments made an impact in past years on the operation of healthcare organizations providing safeguards to protect EHR systems. However, the proliferation of digital health data, trends in data use, increased in the use of telehealth applications, and patient's accesses to their health records all have created new challenges that are not covered by the exiting legal framework established by HIPAA. The U.S healthcare industry continues to operate under a law that was written about two decades ago; thus, financial penalties do not longer seem effective as deterrent to prevent violations to HIPAA laws (Theodos, 2020). Per the literature, as technology continues to advance at a rapid pace along with consumers playing a greater role in the management of their healthcare through digital health the privacy guidance provided by federal law should also shift to reflect the new reality. As the legal framework that protects the privacy of patients' health information, the enforcement of HIPAA regulations could have a significant influence on how healthcare organizations handle and protect EHR data. Under HIPAA, reported non-compliances are submitted for investigation and final ruling determination with some of these investigations resulting in financial penalties to the state organizations (Theodos, 2020).

Questions:

1. How does compliance with government policy (HIPAA) influence management's behavior towards improving information security systems?

2. How effective are monetary penalties influencing the behavior of healthcare organizations' emphasis on compliance with government policy?

3. What recommendations or best practices can be implemented by healthcare organizations looking to strengthen their HIPAA compliance efforts and reduce the risk of human error data breaches?

Appendix G
STS Factors and Subject Matter Experts (SME) for Semi-Structured Interviews

STS Factor	Expertise Field	Subject Matter Expert (SME)
Identify Access Management (IAM)	**Cybersecurity**	A program manager developing an IAM program for protecting national security data
System Diversity	**Cybersecurity**	A cybersecurity system designer developing system countermeasures to prevent data intrusions from unauthorized users
Business Processes	**Healthcare**	A healthcare consultant to government and major healthcare entities in digital transformation of healthcare organizations
Cybersecurity Protocols	**Cybersecurity**	A zero trust compliance manager implementing measures to protect national security data
Human in the Loop	**Healthcare**	A hospital pharmacy director responsible for reviewing patient records with prescriptions; an emergency room physician with daily access to patient records;
User Awareness	**Healthcare**	A healthcare record manager expert with daily EHR interactions at a major healthcare provider, and responsible for maintaining the EHR in a major healthcare system
Regulations	**Policy**	A policy director from a government agency responsible for the development and compliance of cybersecurity policy to protect national security data.

Appendix H
Semi-Structured Interview Results

VIRGINIA TECH

Essays on Human Error in Electronic Health Records (EHR) Information Security

Semi-Structured Interview Results

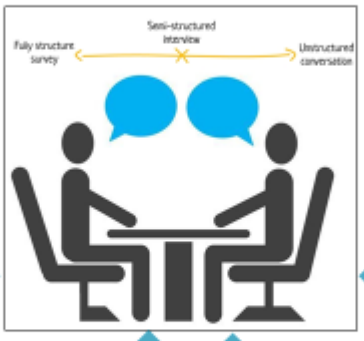
Final Dissertation Outbrief

Wilmer Alvarado
April 2025

1

VIRGINIA TECH

Benefits of Semi-Structured Interviews



Learn about nuances in patient care practices that surveys or literature may not reveal

Enhance other research findings from quantitative research

Obtain opinions from real-world experts in the cyber and healthcare professional fields

Access to real world examples on the impact of human error on healthcare data breaches

2

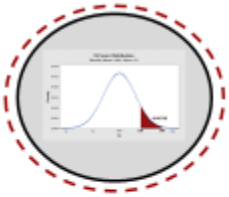
VIRGINIA TECH

Data Collection - Qualitative Data

SEMI-STRUCTURED INTERVIEWS

Receive Feedback
from Subject Matter Experts (SME)

EXPECTED BENEFITS



Inform Methods Development
and Hypothesis Testing

Essay 1:	• Role of Human Error in Data Breaches • Places/Reasons Where Data are Breached
Essay 2:	• Unintended Consequences of Technology • Barriers to EHR Adoption Sharing • Impacts to Healthcare Performance
Essay 3:	• Effectiveness of Policy on EHR Security

3

VIRGINIA TECH

Semi-Structured Interviews with SME

Healthcare

Cybersecurity

Policy

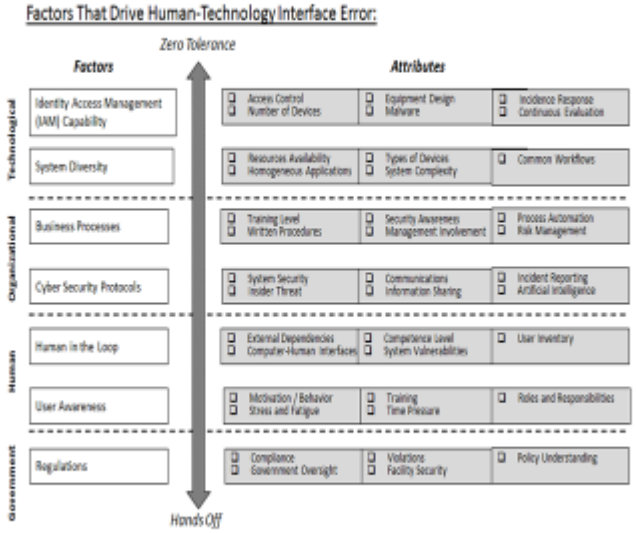
Note: Virginia Tech Institutional Review Board (IRB) determined that the proposed activity is not research involving human subjects as defined by HHS and FDA regulations.

Provide Real World Qualitative Data to Support Research Study

4

VIRGINIA TECH

Socio Technical System (STS) Management Framework



Applies a STS Approach to Information Security of EHR

5

VIRGINIA TECH

Subject Matter Experts (SME) By STS Factors

Obtain Diverse Opinions About Healthcare Information Security

6

VIRGINIA TECH

Essay Interview Objectives and Questions

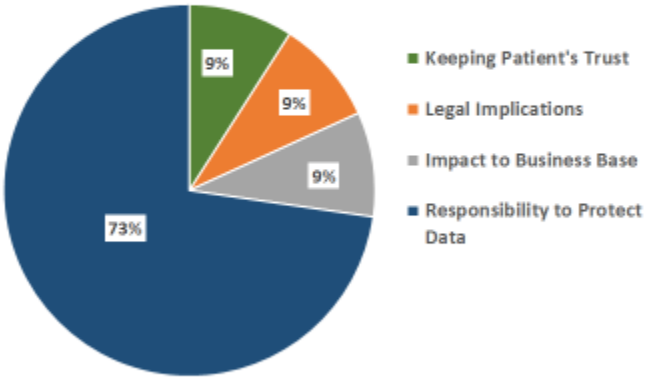
Essay 1: Human Technology Interface Error in Healthcare Data Breaches	Essay 2: Unintended Consequences from Adoption of EHR Technology	Essay 3: Application of Policy as a Safeguard Layer to Reduce Human Error Data Breaches
• Why Organizations Should Care About Cybersecurity? • What are the Most Common Situations Where Human Errors Have Led to Security Breaches? • What STS Factors Have the Most Impact Reducing the Risk of Human Errors?	• Do Security Breaches Affect Organizations' Performance? • How Do Healthcare Professionals Navigate Privacy Concerns? • What are People's Perceptions of Organizations After Privacy Violation Incidents?	• How Does Government Policy Impact Management Behavior to Improve Security Systems? • How Effective are Monetary Penalties in Influencing Government Policy Compliance? • What are the Best Practices to Strengthen Policy Compliance Efforts in Organizations?

7

VIRGINIA TECH

Interview Results – Importance of Cybersecurity

Question: Why Organizations Should Care About Cybersecurity?



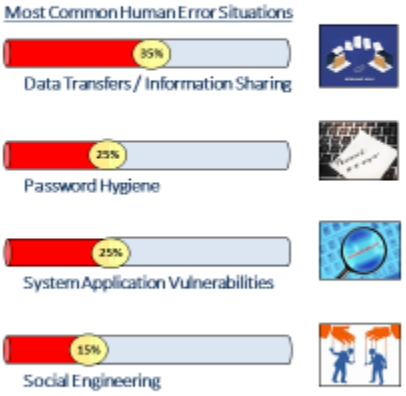
Protection of Data Should be Highest Priority for Healthcare Organizations

8

VIRGINIA TECH

Interview Results – Causes of Data Breach Incidents

Question: What are the Most Common Situations Where Human Errors Have Led to Security Breaches?



Data Transfers and Password Hygiene are the Most Common Human Error

9

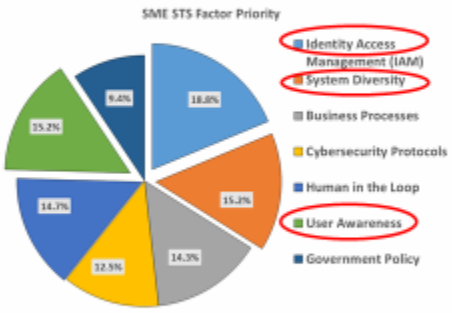
VIRGINIA TECH

Interview Results - STS Factors That Drive Human Error

Question: What STS factors have the most impact reducing the risk of human errors?

STS Factor Ranked by Order of Priority

Subject Matter Expert (SME)	Identity Access Management (IAM)	System Diversity	Business Processes	Cybersecurity Protocols	Human in the Loop	User Awareness	Government Policy
IAM Program Manager	7	6	5	2	3	4	1
Cybersecurity System Designer	6	7	2	3	4	1	5
Healthcare Digital Platform Consultant	1	2	5	4	7	6	3
Zero Trust Compliance Program Manager	7	3	5	6	1	4	2
Hospital Pharmacy Director	4	1	3	2	6	5	7
Emergency Room Physician	7	5	2	4	3	6	1
Healthcare Records Manager	3	6	4	2	7	5	1
Government Policy Manager	7	4	6	5	2	3	1
Score (Highest Priority: 7)	42	34	32	28	30	34	21
Share (%)	18.8%	15.2%	14.3%	12.5%	14.7%	15.2%	9.4%
STS Order of Priority	1st	2nd	5th	6th	4th	2nd	7th



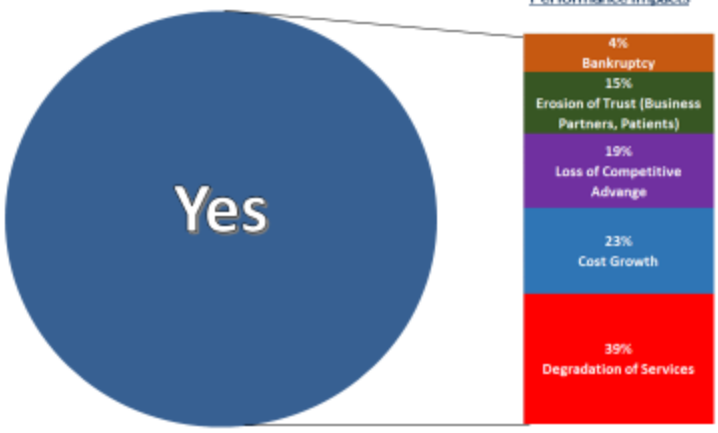
IAM, System Diversity, and User Awareness are the Most Influential STS Factors

10

VIRGINIA TECH

Interview Results – Impact to Performance

Question: Do Security Breaches Affect Organizations' Performance?



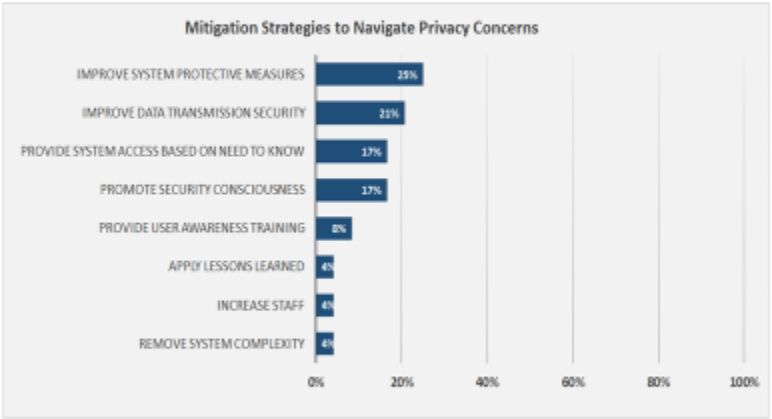
Security Breaches Cause Degradation in Patient Care Services

11

VIRGINIA TECH

Interview Results – Privacy Concerns Mitigation Strategies

Question: How Do Healthcare Professionals Navigate Privacy Concerns?



Improve System Protective Measure and Data Transmission Security

12

VIRGINIA TECH

Interview Results – Perception After Privacy Violations

Question: What are People's Perceptions of Organizations After Privacy Violation Incidents?

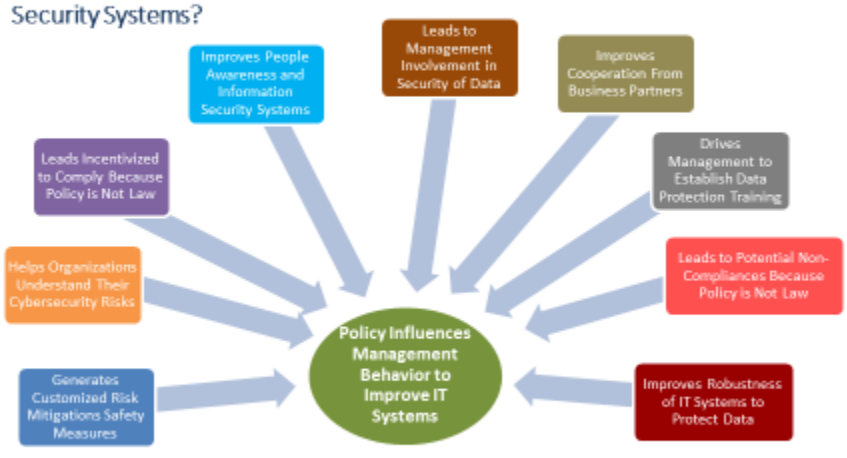
Concerns About Sharing Data but Mixed Opinions About Impact to People's Trust in Organizations

13

VIRGINIA TECH

Interview Results – Influence of Regulatory Measures

Question: How Does Government Policy Impact Management Behavior to Improve Security Systems?



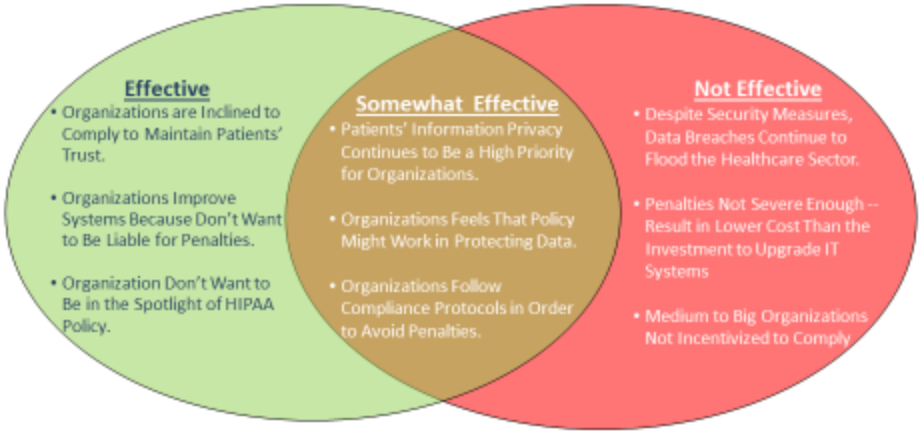
Lead to Improvements in Healthcare IT Systems

14

VIRGINIA TECH

Interview Results – Impact of Monetary Penalties

Question: How Effective are Monetary Penalties in Influencing Government Policy Compliance?



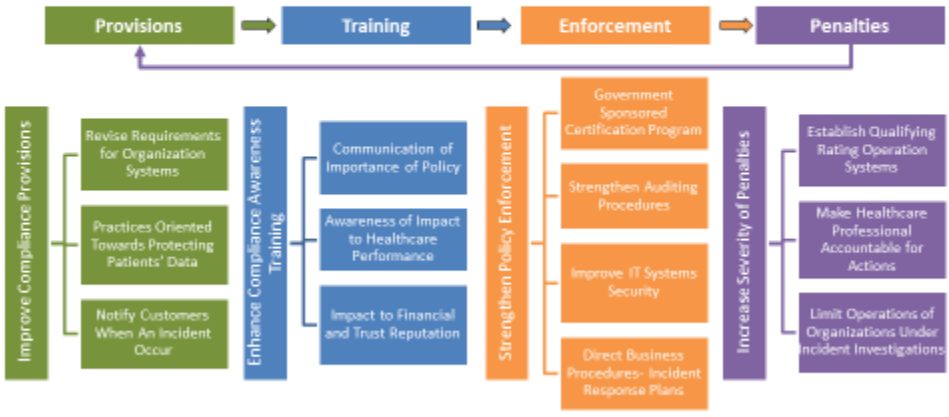
Mixed Results About Effectiveness of Monetary Penalties

15

VIRGINIA TECH

Interview Results – Compliance Best Practices

Question: What are the Best Practices to Strengthen Policy Compliance Efforts in Organizations?



16

VIRGINIA TECH

How Research Focus Relates to Interview Results

Literature Gap	Research Questions Focus	Interview Results
Essay 1: Assess the Impact of STS Factors on the Reduction of Human-Computer Interaction Errors	Importance of Reducing Human Error	• Protection of Data Should Be Highest Priority • Keeping Patient's Trust • Reduce Legal Implications • Impact to Business Base
	Most Common Sources / Locations of Human Error	• Data Transfers • Password Hygiene • System Application Vulnerabilities • Social Engineering
	Most Impactful STS Factors to Human Error	• Identity Access Management (AIM) • System Diversity • User Awareness, and • Human in the Loop
Essay 2: Investigate Impact of Unintended Consequences from Technology Adoption to Patient Care Services	How Information Privacy Concerns Impact Healthcare Performance	Security Breaches Affect Performance: • Cause Degradation in Patient Care Services • Increase Cost Operations for Organizations • Contribute to Loss of Competitive Advantage • Cause Erosion of Trust with Business Partners and Patients
		Mitigation Strategies Include: • Promote System Protective Measures • Limit System Access (Need to Know) • Improve Data Transmission Security
		Perceptions After Privacy Violation: • Mixed Results About Trust in Organization Processes • Create Concerns About Data Sharing
Essay 3: Confirm or Refute the Effectiveness of HIPAA Policy on Healthcare Performance	Effect of HIPAA Policy as a Security Layer on the Healthcare Performance	Policy Influences Management Behavior to Improve IT Security • Improves Users Awareness • Leads to Management Involvement • Improves Cooperation from Business Partners • Introduces Need for Data Protection Training
		Mixed Results About Effectiveness of Monetary Penalties • Comply to Maintain Patients' Trust • Policy Sometimes Work on Protecting Data • Data Breaches Continue to Flood the Sector.
		Best Practices to Strengthen Compliance: • Improve Policy Provisions • Introduce User Training • Create Needs of Policy Enforcement • Increase Severity in Compliance Penalties

17

VIRGINIA TECH

Conclusions - Takeaway

- ***Essay 1: Protection of data should be the highest priority for organizations***
  - Human error data breaches affect business decision with healthcare provider
  - Data transfer and password hygiene are the most common human error
  - Emails and access to network servers are most common locations where data are breached
- ***Essay 2: Security breaches affect performance of healthcare organizations***
  - Cause degradation in patient care services and increase cost of operations
  - Create concerns about information sharing between organizations
- ***Essay 3: Monetary penalties for non-compliance are not severe enough***
  - Paying Penalties Result in Lower Cost Than Organizations' Investment to Correct IT Systems
  - Government entities not allowed to accept ransom from Cyber attackers

Interviews Inform Essays' Hypotheses and Findings from the Literature Review

18

VIRGINIA TECH

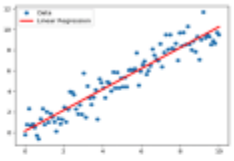
How are the Findings Informs the Research

Interview Takeaways	Qualitative Results	How Findings Inform the Research
Essay 1: Protection of Data Should be Highest Priority	• Provided Insight into Most Common Human Errors and Sources and Locations Where Data are Breached	Location Where Data are Breached • Data Transfers: Emails, Paper Films, EHRs • PW Hygiene: NW Servers, Desktop Computers • System Vulnerabilities: NW Servers • Social Engineering: NW Servers, Emails
Essay 2: Security Breaches Affect Performance of Healthcare Organizations	• Identified Differences in Organizations' System Capability to Protect Data, and Impacts to Cost and Patient Care Services • Provided Insights into Variable Selection for Clustering and Performance Index • Highlighted Impact of Digitization to Performance Improvement	Clustering Variables • Multiple Variables (Demographic, Healthcare Performance Metrics) • Reduction -Principal Component Analysis MPI Variables • Adoption of EHRs • Data Breaches • Patients Managed • GDP per Capita • Healthcare Expenditures/Capita • Total Deaths • Length of Stay • Life Expectancy
Essay 3: Monetary Penalties for Non-Compliance are Not Severe Enough	• Mixed Results about Effectiveness of Monetary Policies • Human Error Data Breaches Continue to Flood the Sector • Policy Sometimes Work on Protecting Data	Regression Variables • Patient Records Compromised • Monetary Penalties Paid • Human Error Data Breach Incidents

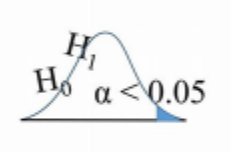
19

VIRGINIA TECH

NEXT STEPS



Use Results to Inform Quantitative Methods and Hypothesis Testing



Conduct Data Analysis and Hypotheses Testing

Formulate Research Conclusions and Future Research Needs.

20

Appendix I
Virginia Tech Institutional Review Board (IRB) - Request Form

Human Research Protection Program
Institutional Review Board
Research Determination Form

VIRGINIA TECH

Instructions:
To assess whether IRB review is necessary for a project, a determination must be made whether the project is research and, if so, whether it involves human subjects. An investigator conducting an activity with or about humans must make a request for a research determination through the IRB Protocol Management System (PMS).

All requests must include a detailed description of the activities and any supporting documents. Once complete, please upload this form as a Word or PDF document to the IRB Protocol Management System (PMS): https://secure.research.vt.edu/irb. A research determination official (either a designated departmental Human Subjects Advisor [HSA] or a Human Research Protection Program [HRPP] staff member) will review your completed request within 2-3 business days. If your project is determined to be not human subjects research (also called NHSR), HRPP will send you a memo that includes the IRB tracking number, which you can provide to journals and funding organizations upon request.

Definitions:

The federal regulations define 'research' and 'human subjects' as follows (please see SOP HRP-001 for the full regulatory language):

Research is defined as a systematic investigation (including research development, testing, and evaluation) designed to develop or contribute to generalizable knowledge.

A ***human subject*** is defined as a living individual about whom an investigator either:
1) Obtains information through intervention or interaction with the individual, or
2) Obtains, uses, studies, analyzes, or generates identifiable private information or identifiable biospecimens.

Outcomes and Next Steps:

If the activity does not meet the definitions of research and/or human subjects, the determination official will issue a "Not Research" or "Not Human Subjects Research" letter and send it to the investigator through the IRB PMS. The investigator can begin the activities upon receipt of this letter.

If the activity does meet the definition of human subjects research, the submission will be returned to the PI with further instructions about how to submit a research protocol for IRB review.

Submissions that do not contain adequate details or information will be returned to the investigator for revision. If you have any questions, you can email us at irb@vt.edu.

* Questions with an asterisk require a response. To avoid delays, please ensure that your submission is complete.

Section 1: General information

1.1 Project title: *

Essays on Human Technology Interface Error in Electronic Health Records (EHR) Information Security

1.2 Principal Investigator (Name): *

Wilmer Alvarado

1.3 Funding information: *

N/a

1.4 Is this a collaborative project?*

☒ No

☐ **Yes – check all the activities Virginia Tech will be involved in with the collaborating institution:**

- ☐ Research design/development
- ☐ Recruitment or dissemination of recruitment materials
- ☐ Consenting participants
- ☐ Data collection
- ☐ Analysis of **identifiable** data or information
- ☐ Analysis of **de-identified** data or information
- ☐ Consultation or manuscript writing

1.5 Is this activity being conducted by a student to meet course work or graduation requirements? *

☐ **No**

☒ **Yes,** please check all that apply.

- ☐ Thesis
- ☒ Dissertation
- ☐ Class assignment/routine coursework
- ☐ Other, please explain below:

The interview sessions will be conducted to inform the questions, hypotheses, and hypotheses testing to meet the requirements of the dissertation work.

Section 2: Is this activity research, as defined by the IRB regulations?

2.1 Is this activity a systematic investigation? *

(Systematic: Having or involving a system, method, or plan. Investigation: A searching inquiry for facts; detailed or careful examination. A systematic investigation is usually recognized by the fact that there is a predetermined and organized method [of data collection and analysis] to study a specific topic, answer a specific question, test a hypothesis, or develop a theory.)

☐ **No**

☒ **Yes**

2.2 Is this activity designed to develop or contribute to generalizable knowledge? *

(Generalizable: Universally or widely applicable. Relates to drawing general conclusions, informing policy, or generalizing findings beyond a single individual or an internal program. Note that publishing or presenting the data is not a sole criterion on which to define generalizable knowledge – non-generalizable knowledge is often published or presented, often as case studies.)

☐ **No**

☒ **Yes**

2.3 Describe the purpose and specific aims or objectives of the project. If your planned activity relates to a protocol previously approved by the Virginia Tech HRPP/IRB, please include the Virginia Tech IRB number(s). *

Please provide a detailed description that includes the purpose or goal of the project, objectives, procedures used to gather information (interviews, surveys, focus groups, etc.), target population, and description of data/samples gathered (datasets, URLS, etc.) If there are procedures that the research team is thinking about implementing, but is unsure if they will, a new determination should be submitted at a later time.

Purpose: The aim of the research is to investigate the impact of human technology interface error in technology adoption and performance of information security systems.

Objectives: The research includes the following three objectives:
- Examine human technology interface error in organization's data breaches
- Measure the impact of human error in technology adoption and the performance of information security systems.
- Measure the performance of government policy as a safeguard to reduce human error

Process and Methods:
- Qualitative Data- Interview sessions with subject matter experts from the fields of cybersecurity; healthcare; and government policy.
- Quantitative Data- Data bases on healthcare data breaches by states' healthcare organizations; electronic health record technology adoption; and Health Insurance Portability and Accountability Act (HIPAA) policy violations. The data sets have been collected from the Department of Health and Human Services (DHHS).
- Methods: Hypotheses will be tested using a combination of methods. These methods include: statistical analysis – regression analysis; benchmarking analysis – Data envelopment analysis and mamquist productivity index; statistical analysis- ANOVA text.

2.4 Please describe how the results will be used. *

The results of the dissertation will be used to expand the knowledge of three theories:
- Human factors theory
- Economic production theory
- Reason's theoretical model of accident causation.

In addition, the results from answering the questions and hypotheses from the dissertation will inform healthcare sector decision about electronic health records technology adoption; help healthcare organizations understand causes of data breaches that risks the patient's health information; assist government policy makers understanding the effect that monetary policy has influencing the behavior of healthcare management for improving their information security systems to avoid incompliance penalties.

Section 3: Does this activity involve human subjects?

3.1 Will you interact, intervene, or observe individuals and collect information (or biospecimens) about them? *
(Intervene: Physical procedures or manipulations of individuals or their environment for research purposes. Interact: Communication or interpersonal contact with the individuals.)

☒ **No,** the information being collected is **NOT** about the individual(s) (e.g., it is about programs, policies, and/or practices that the individual(s) are familiar with).
☐ **Yes,** the information being collected **IS** about the individual(s) (e.g., their own personal thoughts, opinions, attitudes, and/or perception)

3.2 Will you obtain or view any of the following identifiers from or about a living person (from any source or already in your possession)? *
Please review the list in its entirety and check all that apply.

☐ Name
☐ Geographical subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the first three digits of a zip code
☐ Elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and single year of age over 89 as well as all elements of dates (including year) indicative of such age, unless such ages and elements are aggregated into a single category of age 90 or older

☐ Phone numbers
☐ Fax numbers
☐ Electronic mail addresses (e-mail)
☐ Social Security numbers
☐ Medical record numbers
☐ Health plan beneficiary numbers
☐ Account numbers
☐ Certificate/license numbers
☐ Vehicle identifiers and serial numbers, including license plate numbers
☐ Device identifiers and serial numbers
☐ Web universal resource locators (URLs)
☐ Internet Protocol (IP) addresses
☐ Biometric identifiers, including finger and voice prints (audio recording)
☐ Full face photographic or video images and any comparable images (video recording)
☐ Student record number or identification/user name
☐ Student grades or class assignments
☐ Username for online or computer accounts
☐ Any other number, characteristic, or code that uniquely identifies an individual (note this does not mean the unique code assigned by the investigator to code the data). Explain:

☐ Other identifiable information. Explain:

3.3 Will you gather public and/or private data (check all that apply)?

☐ Data are about behaviors that occur in a context in which an individual can reasonably expect privacy, for example that no observation or recording is taking place (private information).

☐ Data were collected for specific purposes in which individuals can reasonably expect that they will NOT be made public, such as student records and medical records (private information).

☒ Data consist of publicly available information, such as news stories, a public-use dataset, or other information accessible to everyone (public information).

3.4 Will you video or audio record or photograph individuals during activities? *

☒ **No**
☐ **Yes**

3.5 Will you generate identifiable private information or identifiable biospecimens by combining data sources? * (Can the investigator readily ascertain an individual's identity by combining available datasets and/or biospecimens?)

☒ **No**
☐ **Yes,** answer question within the table 

IF YES
3.5.a Briefly describe what data sources you will use and from whom you will obtain them:

3.6 Will this project involve only the use of existing de-identified data or biospecimens? *

☒ **No,** go to Section 4
☐ **Yes**

3.6.a Were the de-identified data or biospecimens collected specifically for this study?

☐ **No**
☐ **Yes**

3.6.b Will anyone on the research team be able to readily identify individuals to whom the data or specimens pertain or belong? This includes anyone affiliated with the planned activity who has access to a linkage file or key.

☐ **No**
☐ **Yes**

3.7 Does this activity involve a drug or device? *

☒ **No**, go to Section 4
☐ **Yes**, check all that apply

☐ The project involves the use of a drug in one or more persons other than use of an approved drug in the course of medical practice.

☐ The project involves the use of a device in one or more persons that evaluates the safety or effectiveness of the device.

☐ The project involves data about subjects or control subjects submitted to or held for inspection by FDA.

☐ The project involves data about the use of a device on human specimens (identified or unidentified) submitted to or held for inspection by FDA.

Section 4: Supporting Information

4.1 Please select below all applicable documents related to this activity. Please upload a copy of the document(s) (section 4, supporting docs) when you submit this form to IRB PMS. These documents will help us evaluate whether your activity needs HRPP or IRB review. *

If you do not currently have these documents, you can include a brief overview or type(s) of information that will be included.

- ☐ **Grant**
- ☐ **Proposal**
- ☐ **Contract**
- ☐ **Statement of work**
- ☐ **Survey/questionnaire**
- ☒ **Interview/focus group guide**
- ☐ **Observation data sheet**
- ☐ **Other**, please specify:

Section 5: Additional information

5.1 Please provide additional information or instructions that might assist with this review:

No further information.

Proposed modifications to activities must be reviewed by the HSA/HRPP reviewer prior to implementation.

Do not begin activities until you receive an HSA/HRPP determination letter via email.

----------END----------

Appendix J
Virginia Tech Institutional Review Board (IRB) - Approval

Division of Scholarly Integrity and Research Compliance
Institutional Review Board
North End Center, Suite 4120 (MC 0497)
300 Turner Street NW
Blacksburg, Virginia 24061
540/231-3732
irb@vt.edu
http://www.research.vt.edu/sirc/hrpp

MEMORANDUM

DATE: March 20, 2024

TO: Konstantinos P Triantis, Wilmer Alvarado

FROM: Virginia Tech Institutional Review Board (FWA00000572)

PROTOCOL TITLE: Essays on Human Technology Interface Error in Electronic Health Records (EHR) Information Security

IRB NUMBER: **23-968**

Based on the Amendment application, the submitted project description, and items listed in the Special Instructions section found on Page 2, the Virginia Tech Institutional Review Board (IRB) has determined that the proposed activity is not research involving human subjects as defined by HHS and FDA regulations.

Further review and approval by the Virginia Tech Human Research Protection Program (HRPP) is not required because this is not human research. This determination applies only to the activities described in the submitted project description and does not apply should any additional changes be made. If additional changes are made you must immediately submit another Amendment to the HRPP for a new determination. Your amendment must include a description of the changes and you must upload all revised documents. At that time, the HRPP will review the submission activities to confirm the original Not Human Subjects Research" decision or to advise if a new application must be made.

If there are additional undisclosed components that you feel merit a change in this determination, please contact our office for a consultation.

Please be aware that receiving a "Not Human Subjects Research" Determination is not the same as IRB review and approval of the activity. You are NOT to use IRB consent forms or templates for these activities. If you have any questions, please contact the Virginia Tech HRPP office at 540-231-3732 or irb@vt.edu.

PROTOCOL INFORMATION:

Determined As: **Not Human Subjects Research**
Protocol Determination Date: **September 29, 2023**

ASSOCIATED FUNDING:

The table on the following page indicates whether grant proposals are related to this protocol, and which of the listed proposals, if any, have been compared to this protocol, if required.