BMC Health Services Research

RESEARCH

Open Access

The U.S. health system vulnerabilities

Nataliya D. Brantly[1*]

Abstract

Background The increasing integration of health information technology (health IT) into the U.S. healthcare system has brought both opportunities for improvement and new vulnerabilities. The 2024–2030 Federal Health IT Strategic Plan emphasizes equitable data access, quality representative data, and the responsible use of artificial intelligence (AI) to improve health outcomes. Yet, the growing complexity of digital infrastructures has amplified risks related to privacy and the security of protected health information (PHI). This study examines U.S. health system vulnerabilities by analyzing reported PHI breaches and situating them within evolving federal health IT priorities.

Methods This mixed-methods descriptive study combines quantitative analysis of the U.S. Department of Health and Human ServiCE's (HHS) Breach Portal data (2013–2023) with a qualitative review of federal policy and regulatory developments related to health IT. Breaches of PHI affecting more than 500 individuals were included, consistent with HHS reporting requirements. Duplicate and incomplete entries were removed. Breaches were categorized by cause and type. Quantitative results describe frequencies, proportions, and trends, while qualitative analysis of policy documents and breach narratives contextualizes these findings within the broader framework of digital health governance.

Results From 2013 to 2023, the total number of reported PHI breaches and the share attributed to hacking and IT incidents increased markedly, while those involving theft, loss, or improper disposal declined. Healthcare providers accounted for most reported breaches, followed by business associates and health plans. Despite advances in interoperability and automation, the healthcare sector remains disproportionately affected by cybersecurity incidents. The qualitative analysis reveals persistent gaps between federal strategic goals and the practical implementation of privacy and security safeguards across healthcare.

Conclusion This study underscores the paradox of digital transformation: while health IT adoption improves efficiency, coordination, and data sharing, it simultaneously exposes the healthcare system to new risks. Strengthening system resilience requires harmonized governance, continuous monitoring, and greater investment in digital literacy. As AI use and automation expand, policy reforms must ensure that innovation does not compromise patient privacy or deepen inequities. These findings contribute to a better understanding of health system vulnerabilities and offer insights for enhancing the security and resilience of the U.S. health system.

Keywords Digital health, Healthcare, Health system, Electronic, Security, Health IT

*Correspondence:
Nataliya D. Brantly
nbrantly@vt.edu
[1]Government & International Affairs (GIA), School of Public and International Affairs, Virginia Polytechnic Institute and State University, 223 Major Williams Hall, 220 Stanger Street, Blacksburg, VA 24061, USA

Introduction

In September 2024, the U.S. Department of Health and Human ServiCE's (HHS) announced the publication of the 2024–2030 Federal Health IT Strategic Plan outlining federal goals and objectives for health information technology (health IT) development [1]. The plan reflects a collaborative effort of federal and non-federal stakeholders. It reflects the mission of federal health IT to "improve the health and well-being of individuals and communities using technology and health information that is accessible when and where it matters most" [2]. While the previous strategic plan of 2020–2025 focused on promoting health IT infrastructure and addressing barriers to the access, exchange, and use of electronic health information, the current plan recognizes the need for high-quality representative data and commits to improving data access, especially for the development and use of data-driven Artificial Intelligence (AI) technologies. These evolving priorities signal the growing reliance on digital infrastructures and the simultaneous need to safeguard sensitive health data.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 established federal standards to protect sensitive health information from disclosure without a patient's consent. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 incentivized the adoption and meaningful use of health IT and strengthened HIPAA's privacy and security provisions. Under Section 13402 of the HITECH Act, covered entities and their business associates [3] must report breaches of unsecured protected health information (PHI) affecting 500 or more individuals to HHS. In this case, breach means an "unauthorized acquisition, access, use, or disclosure of protected health information," except when the recipient could not reasonably retain the information [4].

PHI is considered to be an "individual's health, treatment, and payment information, and any further information maintained in the same designated record set that could identify the individual or be used with other information in the record set to identify the individual" [5]. Such a definition of PHI is very broad and includes a variety of information patients share with health providers (family health history, demographic information, employment data, and financial information) and information produced by the health provider (clinical notes and medical testing results). Data that constitute PHI can be conceptualized as data at rest (data storage in databases and file systems), data in use (in the process of being created, accessed, updated, deleted), data in motion (data moving through a digital network or physically transported), and data disposed of (recycled electronic devices, discarded paper records). Each data state poses vulnerabilities and requires different approaches to security.

The National Institute of Standards and Technology (NIST) recommends safeguards for securing PHI, including encryption and data destruction protocols to make PHI unusable, unreadable, or indecipherable to unauthorized actors [6]. Despite these guidelines, the complexity of the healthcare ecosystem, comprising diverse covered entities that collect, produce, store, and transmit PHI, creates persistent risks of unauthorized access and misuse. Moreover, the HITECH Act's requirement for entities to determine their own reasonable and appropriate safeguards introduces substantial variation in implementation and oversight [7].

Amid rapid digital transformation, federal health priorities emphasize not only expanding health IT infrastructure while reducing barriers and inequalities, but also enhancing data quality and integrating AI-driven automation. Yet researchers warn that these advances can amplify vulnerabilities in privacy, security, and governance [8, 9]. Understanding the empirical dimensions of these vulnerabilities is crucial for designing effective policy interventions.

This study addresses this gap through a mixed-methods descriptive analysis of PHI breach reports submitted to HHS from 2013 to 2023. By juxtaposing federal strategic objectives with real-world trends in data security incidents, the paper examines how the evolving U.S. health IT landscape simultaneously resolves certain challenges and introduces new systemic risks. The analysis contributes to broader discussions of health system resilience, digital governance, and the unintended consequences of healthcare automation.

The paper proceeds in five sections. The first section presents the methods, detailing the quantitative and qualitative components of the analysis. The second section reviews relevant scholarship and regulatory frameworks on health data governance and privacy protection. The third section reports key findings, and the fourth section discusses their implications for federal health IT policy and system resilience. The paper concludes with recommendations for strengthening cybersecurity governance and directions for future research.

Methods

Study design and data source

This study employs a mixed-methods design integrating quantitative analysis of data breaches involving unsecured PHI reported to HHS from 2013 to 2023 with a qualitative review of federal policy and regulatory developments related to health IT. The primary data source is the HHS Office for Civil Rights (OCR) Breach Portal, which publicly lists breaches affecting 500 or more individuals in accordance with Section 13402(e)(4) of the HITECH Act. The dataset includes information on the covered entity name, entity type, number of individuals

affected, breach submission and reporting dates, location and type of breach, and brief narrative descriptions.

Data preparation criteria

Data were downloaded from the HHS Breach Portal in Excel format and manually reviewed for completeness and consistency. Data were analyzed using JMP Pro 18 software. In alignment with HHS reporting standards, only breaches involving 500 or more individuals were included in this analysis. When necessary, textual inconsistencies were standardized, for instance, harmonizing variations in breach-type terminology (e.g., "Unauthorized Access/Disclosure" vs. "Unauthorized Disclosure"). Duplicate reports were identified through matching entity names, reporting dates, and breach descriptions, and subsequently removed. Entries lacking essential fields (e.g., breach type, number of individuals affected, or reporting date) were excluded to ensure data quality and analytic consistency. Entries indicating the case was consolidated into an existing compliance investigation, entity reporting was not a covered entity, and the event was determined not to be a breach were also excluded. Below is an example of the breach description that led to the exclusion of a data point:

> *On October 21, 2017, the Recovery Institute of the South East, P.A., the covered entity (CE), reported that a former employee remotely accessed its computers without authorization between December 2016 and October 2017. The CE reported that 689 individuals were affected; however, a subsequent forensic investigation by Envista Forensics found no evidence of malware, unauthorized access, or unauthorized data exfiltration. Based on these findings, the CE concluded that protected health information (PHI) was not exposed, and no patients were affected.*

Data analysis and analytic integration

Quantitative analysis was conducted using descriptive statistics to summarize breach characteristics and identify temporal trends. The quantitative analysis aimed to provide an empirical overview of systemic vulnerabilities within the U.S. healthcare system as reflected in HHS breach reporting data. To complement the quantitative findings, a qualitative content analysis was conducted on the narrative breach descriptions provided in the HHS dataset, as well as on selected regulatory documents and guidance issued by HHS and the Office for the National Coordinator for Health Information Technology (ONC). The breach narratives, which detail the nature and context of each incident, were reviewed to identify recurring themes related to security lapses, human error, and systemic weaknesses. In parallel, relevant policy documents were examined to assess regulatory framing, evolving enforcement priorities, and language surrounding accountability and compliance. The integration of these two qualitative data sources allowed for a nuanced understanding of how federal health IT policies intersect with the real-world challenges of protecting PHI.

Regulatory framework protecting health data Today

The U.S. healthcare system has undergone digitalization, driven by the implementation of health IT to improve the overall system efficiency, effectiveness, quality, and safety. These processes have been guided by regulatory and legislative incentives and requirements. While digitalization has generated measurable benefits for healthcare providers and systems, it has also introduced new complexities, responsibilities, and risks for providers, regulators, and patients alike. Federal health IT policy is based on the well-documented findings pertaining to the systemic failures in U.S. healthcare, including system complexity, fragmentation, inefficiencies, poor coordination, and inadequate patient-centric care [10]. Reports of thousands of annual deaths due to medical errors in a clinical setting highlight the need to focus on patient safety as a fundamental priority and to reform the healthcare system to one focused on safety [11]. Moreover, U.S. healthcare spending remains the highest globally [12], more than twice the average per person spending of other high-income countries [13], exceeding $4.9 trillion or $14,570 per person in 2023 [14]. Policymakers continue to look toward automation to address these issues and to eliminate inefficiencies.

Early evidence suggests that health IT can enhance care quality and efficiency. Hillestad et al. demonstrated that selective implementation of health IT improved surveillance, reduced medication errors, and yielded clear advantages of electronic health records (EHR) systems over paper-based systems [15]. The widespread adoption of EHR was estimated to result in annual savings of $81 billion, with the potential to double these savings by utilizing health IT to prevent and manage chronic conditions [16]. Yet, adoption remained low for many acute care hospitals as of 2008, despite the consensus that health IT use should result in "more efficient, safer, and higher-quality care" [17], prompting the federal government to encourage the adoption of EHR systems.

Federal efforts to promote health IT adoption include a range of financial, regulatory, and technical initiatives. The American Recovery and Reinvestment Act of 2009 offered financial support for EHR adoption and maintenance [18]. Concurrently, the Centers for Medicare and Medicaid ServiCE's (CMS) implemented penalties for eligible entities and professionals for failing to demonstrate "meaningful use" of a certified EHR system by 2015, evolving into the Medicare Promoting Interoperability

Program [19]. The Office of the National Coordinator for Health Information Technology (ONC) leads the health IT certification program, including EHRs [20], and supports the workforce development and training programs nationwide [21].

Despite these initiatives, digital health technologies have yet to realize their promise of safer, higher quality, and lower cost care [22, 23]. Health IT adoption places additional burdens on healthcare providers due to implementation, documentation, and configuration issues, contributing to clinician burnout [24, 25]. Integration difficulties, workflow disruptions, and usability challenges remain persistent concerns. Early federal policies prioritized adoption and meaningful use over workflow optimization or provider well-being, leaving systemic issues of interoperability, governance, and resource allocation only partially addressed [26].

The complexity of health IT implementation extends across multiple stakeholders, including providers, regulatory agencies, insurance payers, and health IT vendors. The HITECH Act of 2009 applies not only to covered entities but also to their business associates, entities that provide "legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services" involving PHI [27]. Estimates suggest that covered entities spend most of their IT budgets on the implementation of new technologies (around 95%), while less than 5% goes to security, contributing to persistent gaps in PHI protection compared to other leading industries [28].

Modernization efforts, including the 21st Century Cures Act of 2016, have emphasized security, interoperability, and the reduction of provider burden [29]. Agencies such as the ONC and the Agency for Healthcare Research and Quality (AHRQ) have focused on improving system usability, implementation, and safety through human factors approaches and targeted research funding [30]. Federal oversight of health IT and data security is distributed across multiple agencies, including HHS (HIPAA enforcement, health IT), the Federal Trade Commission (consumer health data), the U.S. Food and Drug Administration (medical device security), and the Cybersecurity and Infrastructure Security Agency (critical infrastructure protection).

The regulatory framework protecting health data in the U.S. today consists of the following key federal laws that address privacy, security, and patient rights: HIPPA of 1996, the HITECH Act of 2009, and the Cures Act of 2016. Additionally, the Federal Trade Commission (FTC) enforces data privacy for non-HIPAA-covered entities (health apps, fitness trackers, direct-to-consumer genetic testing) through the FTC Act [31] and Health Breach Notification Rule [32]. However, the rapid pace of digitalization of healthcare creates persistent challenges for data accuracy, security, and interoperability. As one report notes, "[t]he speed of innovation in the digital health market requires us to justify a need to establish standards around the technology" [33]. Federal regulations increasingly emphasize network reliance, leaving healthcare organizations responsible for safeguarding vast quantities of PHI in highly interconnected systems [28].

The following analysis uses HHS breach data to provide empirical insights into these vulnerabilities and to contextualize emerging challenges within the current regulatory landscape. As healthcare providers and organizations shifted to digital systems, vulnerabilities to cybersecurity breaches grew. The healthcare industry is an attractive target for criminals who want to access the personal, health, and financial information stored in digital systems [34]. Federal priorities, including those outlined in HHS strategic plans, highlight the importance of both improving access to health IT and securing sensitive data. While the U.S. regulatory framework is focused on patient safety and data protection, it does not limit the collection or use of health data [35]. The following analysis uses HHS breach data to provide empirical insights into these vulnerabilities and to contextualize emerging challenges within the current regulatory landscape.

Results: changing trends in health systems privacy and security 2013–2023

From the beginning of 2013 through the end of 2023, 4,994 breaches of unsecured PHI were reported to the HHS Secretary by covered entities and business associates, impacting over 461.7 million individuals [36]. To ensure data accuracy, the final analytic dataset included 4,186 reported breaches, impacting a total of over 387.7 million individuals from 2013 through the end of 2023. Fig. 1 below displays the steady increase in the number of reported PHI breaches, while Fig. 2 illustrates the corresponding rise in the number of affected individuals.

Subsequently, the PHI data were categorized into three types of data, personal data, financial data, and health data, to determine what type of data was involved in the reported breaches. This categorization determined that 100% of the breaches included personal data, 21.9% included financial information, and 86% included health data, as indicated in Table 1 below.

The dataset revealed that some breaches of unsecured PHI occurred due to a threat emanating from an outside source, and some were internal to the reporting entity. Some of the internal threats include access to data by unauthorized individuals (employee/family member), improper disposal of data, misplaced data, data exposed in error, data theft, and fraudulent use of data by employees of the covered entity. The following is an example of an internal threat:

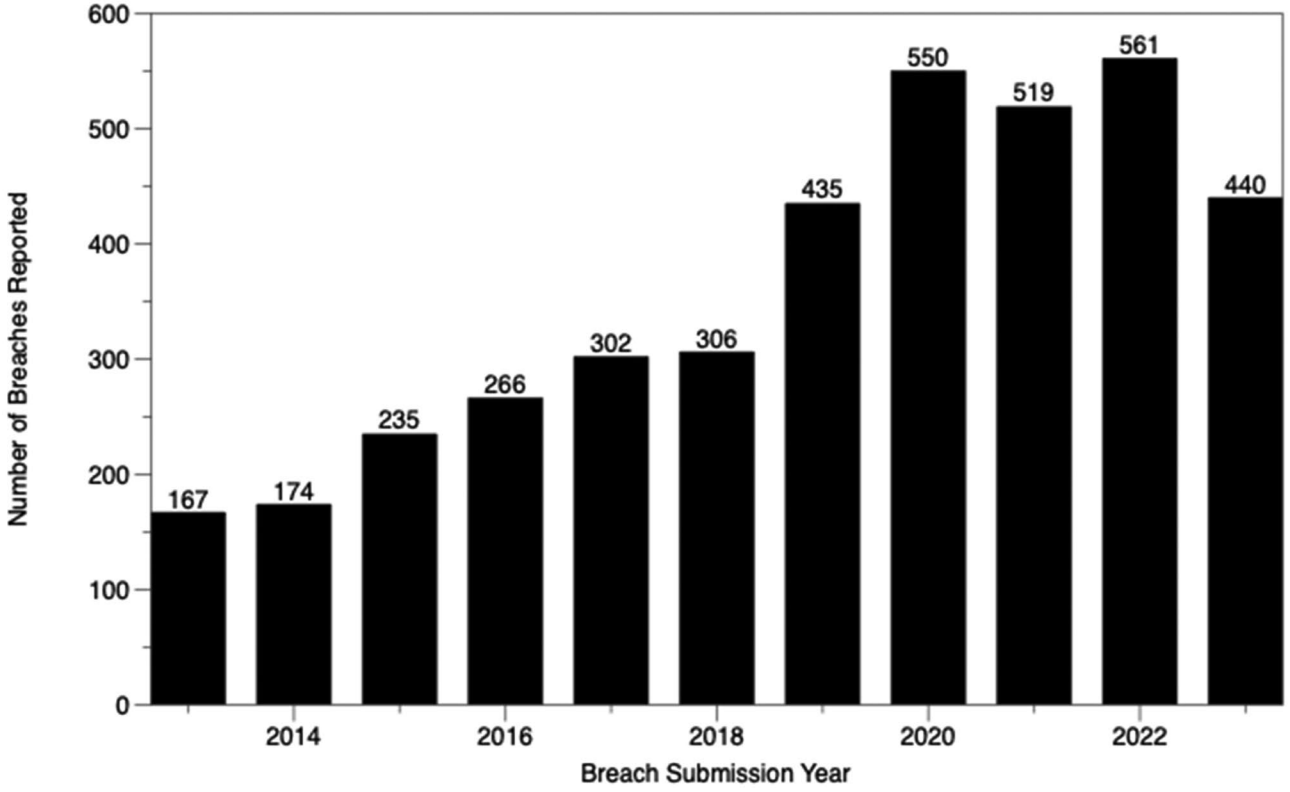

Fig. 1 Number of reported breaches of unprotected PHI annually, 2013–2023

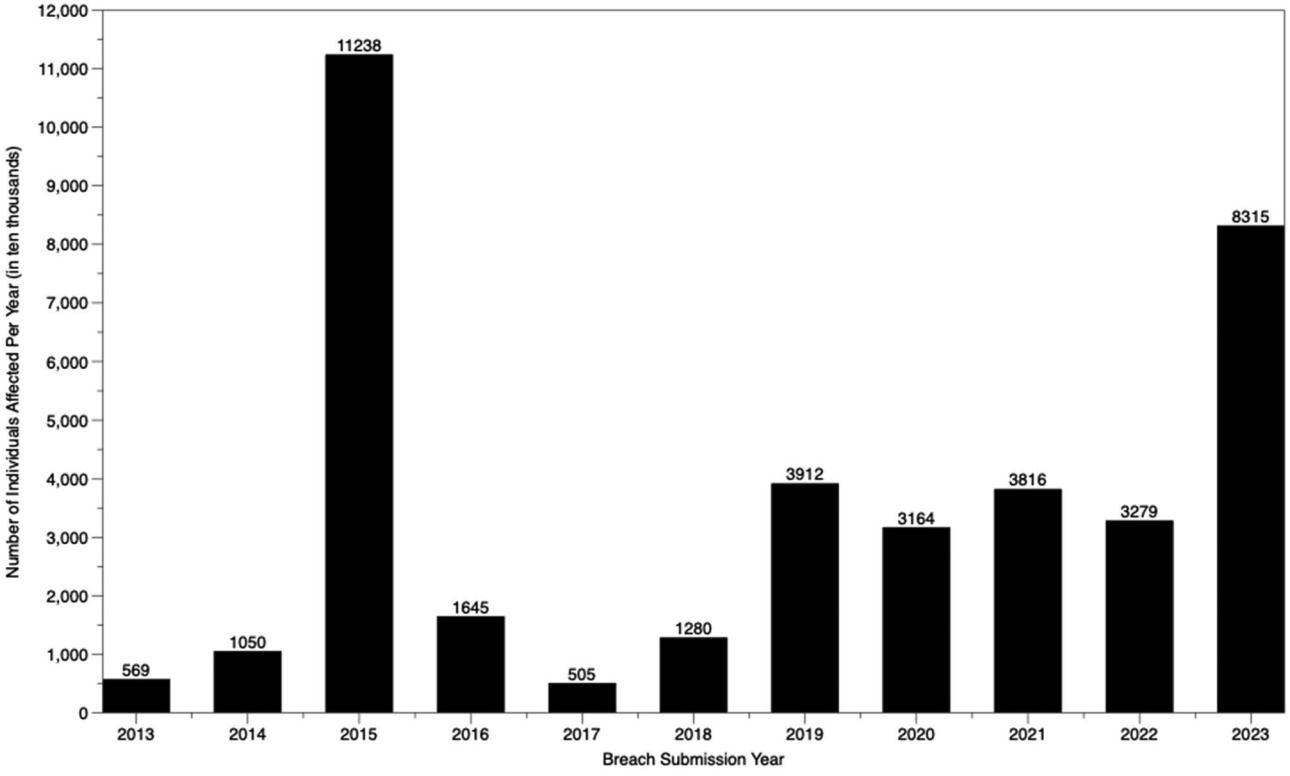

Fig. 2 Number of individuals affected through breaches of unprotected PHI annually, 2013–2023

Table 1 Percent of PHI breaches reported to HHS per data type, 2013–2023

Breached Data Type	Examples of Data	% of Breaches Impacted
Personal Data	Non-medical data: names, home addresses, driver's license information, SSN, contact information, demograPHIc data (age, race, ethnicity, gender, marital status, income, education, payment, etc.), dependents information, emergency contact data.	100%
Financial Data	Payment information (credit card/bank account information), the amount paid, billing history, income verification information.	21.9%
Health Data	Health insurance information, claims, procedures performed, diagnosis data, medications prescribed, medical testing results (lab results).	86%

Table 2 Percent of PHI breaches reported per threat type, (internal vs external), 2013–2023

Threat Type	Example of Threat	% of Breaches Impacted
Internal	Access to data by unauthorized individuals (employees/family members), Improper disposal of data, Misplaced data by employee, Data exposed in error by employee, Data theft and fraudulent by employees of the covered entity.	2013–2023–32.3% 2023–20.0% 2022–18.2% 2021–19.3% 2020–24.1% 2019–29.5% 2018–43.5% 2017–42.8% 2016–50.7% 2015–52.3% 2014–59.3% 2013–55.4%
External	Ransomware attacks, Email PHIshing, Social engineering attacks, Digital data breaches, Cyberattacks, Burglaries, Theft of paper records, Significant weather events, Third-party technology or software issue.	2013–2023–67.7% 2023–80.0% 2022–81.8% 2021–80.7% 2020–75.9% 2019–70.5% 2018 - 56.5% 2017–57.2% 2016–49.3% 2015–47.7% 2014–40.7% 2013–44.6%

On June 5, 2014, the covered entity (CE) reported that a trusted physician who had worked in the office for four years left, and prior to leaving, copied patients' demograPHIc information, including names, social security numbers, addresses, dates of birth, phone numbers, emails, insurance information, and recall dates. The protected health information (PHI) of 5,845 individuals was affected by the breach.

Instances of external threats include ransomware attacks, email PHIshing, social engineering attacks, digital data breaches, cyberattacks, burglaries, and even significant weather events like tornadoes. Below is an example of an external threat, followed by Table 2 summarizing the percent of breaches annually and Figs. 3 and 4 illustrating the change over time per threat type (internal vs external).

On November 13, 2015, the Federal Bureau of Investigation (FBI) informed the covered entity (CE), Maine General Health, that during an ongoing criminal investigation it discovered the CE's data on an online Russian message board. Certain devices storing the CE's data were infected during internet-browsing activity from one of the CE's workstations, allowing an intruder to remotely scan the CE's network, obtain credentials, and thereafter Access the CE's computer servers and workstations containing the protected health information (PHI) of approximately 120,247 individuals.

A further distinction between cyber and non-cyber-related breaches highlights the shift from physical to digital vulnerabilities. Cyber breaches include the following: improper web security, cyber-attacks (ransomware, email PHIshing, brute force attack), computer and software errors, and social engineering attacks. Non-cyber breaches include instances of lost written records or technologies containing PHI (unencrypted USB drives, hard drives), data loss dues to employee actions (unauthorized access to physical files or their disclosure, improper disposal, fraud), lost records via mail, and burglary. Below is an example of the cyber-PHI breach, followed by Table 3 summarizing data and Figs. 5 and 6 based on the cyber or non-cyber-related breach type.

On March 17, 2015, PBC filed a breach report on behalf of itself and its network of affiliates stating that cyber-attackers had gained unauthorized access to its information technology (IT) system. The hackers used a phishing email to install malware that gave them access to PBC's IT system in May 2014, which went undetected for nearly nine months until January 2015. This undetected cyberattack, otherwise known as an advanced persistent threat, resulted in the disclosure of more than 10.4 million individuals' protected health information, including their names, addresses, dates of birth, email addresses, Social Security numbers, bank account information, and health plan clinical information. OCR's investigation found systemic noncompliance with the HIPAA Rules, including failure to conduct an enterprise-wide risk analysis and failures to implement risk management and audit controls.

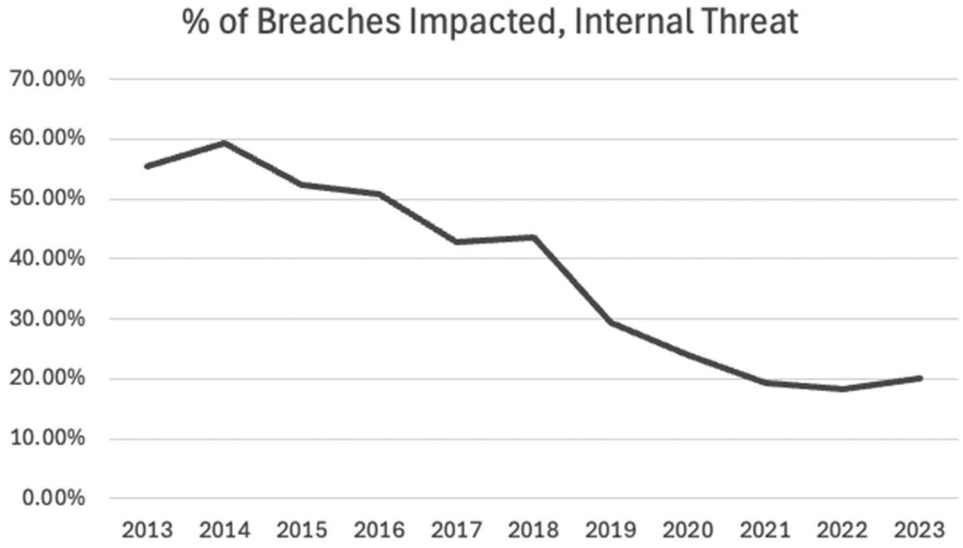

Fig. 3 Percent of PHI breaches impacted by internal threat type, 2013–2023

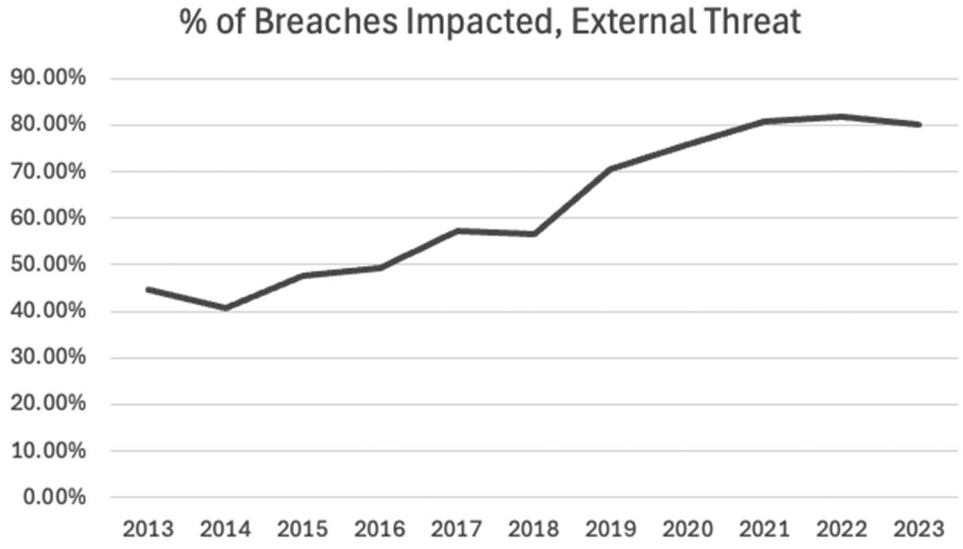

Fig. 4 Percent of PHI breaches impacted by external threat type, 2013–2023

From all the breaches analyzed from 2013 through 2023, 30.3% involved business associates. Those entities that provide legal, accounting, consulting, data analysis, management, administrative, accreditation, financial, and other services to covered entities (hospitals and clinics) have access to PHI. In addition to important privacy and security implications for the individuals whose data was impacted by the breach, the covered entities and their business associates might suffer consequences such as the loss of business, declaration of bankruptcy, or costly payouts/fines if data is not properly secured. Below are a few examples of such instances.

The covered entity (CE), Atchafalaya Internal Medicine Associates, reported a malware attack on its desktop computers that may have compromised the protected health information (PHI) of 2000 patients … On March 6, 2018, OCR received notification from the owner of Atchafalaya Internal Medicine Associates that all healthcare business activities for the entity have ceased, and the entity is no longer operating as a business. OCR verified that the office telephone number is out of service and the entity's website no longer exists … Under these circumstances, Atchafalaya Internal Medicine Associates is no longer a covered entity and is not subject to the requirements of HIPAA.

Table 3 Percent of PHI breaches reported per threat type, (cyber vs non-cyber), 2013–2023

Threat Type	Example of Threat	% of Breaches Impacted
Cyber	Improper web security	2013–2023–59.5%
	Cyber-attacks (ransomware, email phishing, brute force attack)	2023–79.2%
		2022–81.4%
		2021–77.9%
	Computer and software issues, social engineering attacks	2020–69.4%
		2019–63.6%
	Third-party tracking technology	2018–47.1%
		2017–47.0%
		2016–38.3%
		2015–22.7%
		2014–20.9%
		2013–15.3%
Non-Cyber	Lost written records	2013–2023–40.5%
	Lost technologies containing	2023–20.8%
	PHI Data loss dues to employee actions (unauthorized	2022–18.6%
		2021–22.1%
	Access to physical files or their disclosure, improper disposal, fraud)	2020–30.6%
		2019–36.4%
		2018–52.9%
	Lost records via mail	2017–53.0%
	Burglary and theft by employee	2016–61.7%
		2015–77.3%
	Significant weather events	2014–79.1%
		2013–84.7%

The Vein Doctor, the covered entity (CE), reported a breach incident. While attempting to follow up on the breach report, OCR discovered that The Vein Doctor had ceased operations and closed its business. This was verified with the State of Missouri. As of result, the case was closed.

On March 2, 2016, Santa Fe Medical Group/Atrinea Health filed for a Chapter 7 bankruptcy petition and provided OCR documentation of such petition. Under these circumstances Santa Fe Medical Group/Atrinea Health is no longer a covered entity and is not subject to the requirements of HIPAA.

Premera Blue Cross (PBC) has agreed to pay $6.85 million to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human ServiCE's (HHS) and to implement a corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules related to a breach affecting over 10.4 million people. This resolution represents the second-largest payment to resolve a HIPAA investigation in OCR history. PBC operates in Washington and Alaska, and is the largest health plan in the Pacific Northwest, serving more than two million people.

The involvement of third-party vendors and third-party technologies, the first instances of which appeared in the second half of 2022 within the data analyzed, adds to the complexity of PHI protection, as exemplified by the following two breach descriptions.

The covered entity (CE), Novant Health, reported that a tracking pixel on its website may have allowed the protected health information (PHI) of 1,362,296 individuals to be transmitted to Meta. The PHI involved include email addresses, computer IP addresses, phone numbers, medications, and other treatment information. The CE notified HHS, affected individuals, the media, and posted substitute notice on its website. In response to the breach, the CE implemented additional technical safeguards, revised its policies and procedures, and

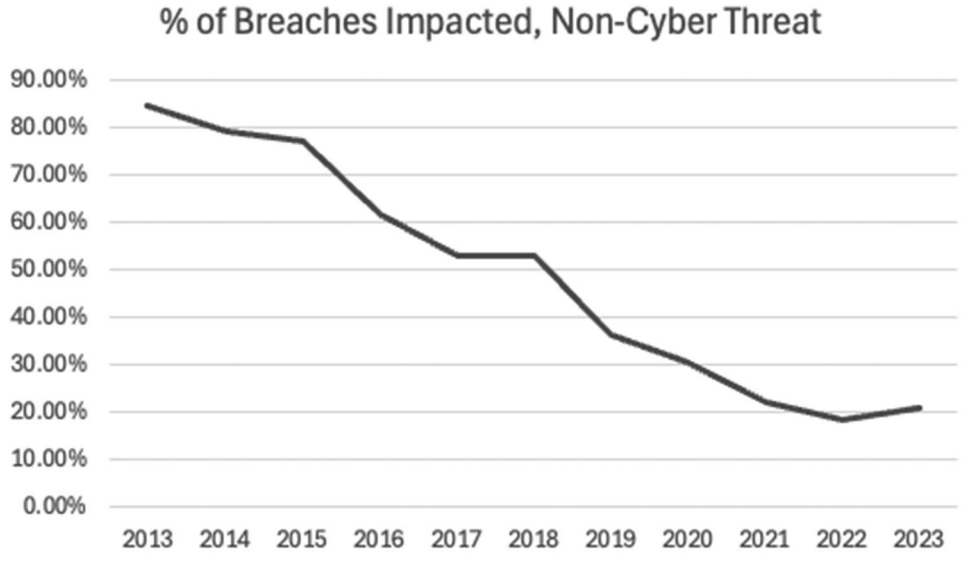

Fig. 5 Percent of PHI breaches impacted by non-cyber threat type, 2013–2023

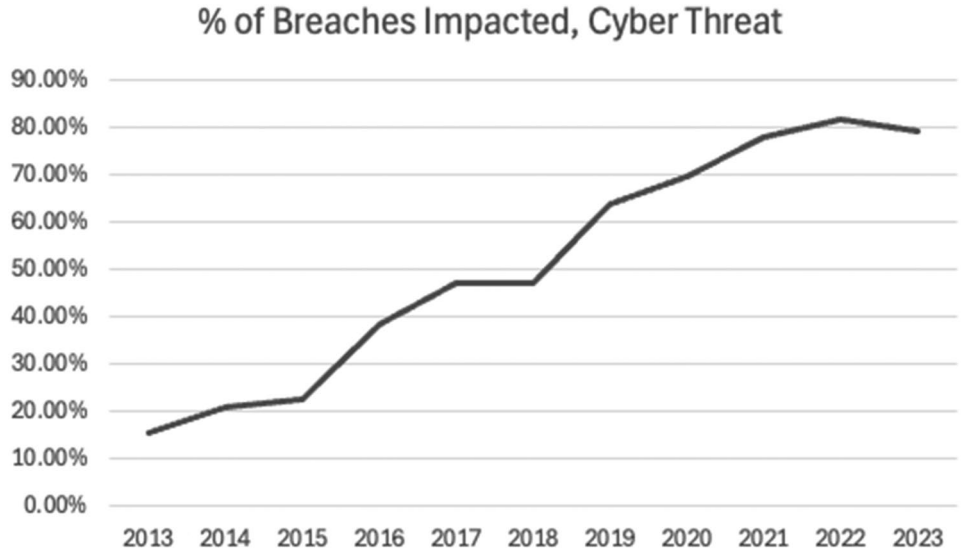

Fig. 6 Percent of PHI breaches impacted by cyber threat type, 2013–2023

provided complimentary credit monitoring services. OCR provided the CE with technical assistance regarding the HIPAA Breach Notification Rule. (Breach Submission Date: 08/14/2022)

OCR opened a compliance review into the covered entity (CE), Community Health Network, due to its potential use of online tracking technology. In response to the compliance review, the CE determined that the protected health information (PHI) of 1,500,000 individuals was impermissibly disclosed to third-party tracking technology vendors, such as Facebook and Google. The PHI involved included names, health insurance information, IP addresses, and treatment information. The CE notified HHS, affected individuals, the media, and provided substitute notice. In response to the breach, the CE ceased using online tacking technology and implemented additional administrative and technical safeguards. (Breach Submission Date: 01/13/2023)

Entities reporting the breaches of unsecured PHI are also responsible for notifying the affected individuals. However, the information provided in such notifications is not sufficient to fully understand the impact of the breach and the risks involved in having patients' PHI accessible to unauthorized actors. Furthermore, covered entities are not required to report the outcome of the investigation that follows a breach of unprotected PHI to affected individuals. In some instances, the outcomes of the investigation can be staggering, as exemplified by the below breach descriptions.

The covered entity (CE), Sheet Metal Local 36 Welfare Fund, reported that an employee of its business associate (BA), People Resources Corporation, inadvertently uploaded Excel spreadsheets containing the CE's Member Assistance Program (MAP) eligibility data onto an unsecure website maintained by the BA. An unknown individual or entity believed to be in China uploaded the data to two additional websites. In addition, two other websites contained links to the BA's unsecure website. The spreadsheets contained the names, addresses, dates of birth, and social security numbers of 4,560 members (but not dependents) … (Breach Submission Date: 07/15/2013)

Prisma Health-Midlands, the covered entity (CE), reported that an employee's computer access credentials were posted for sale on the dark web causing a potential disclosure of the electronic protected health information (ePHI) of 19,060 individuals. The ePHI involved included names, dates of birth, Social Security numbers, addresses, and health insurance information. The CE notified HHS, affected individuals, and the media. In its mitigation efforts, the CE sanctioned the responsible employee and implemented additional technical and security safeguards to better protect its sensitive data. The CE offered complimentary credit monitoring services to affected individuals. OCR obtained assurances that the CE implemented the corrective actions noted. (Breach Submission Date: 10/28/2019)

Lastly, on March 13, 2015, Anthem, Inc., a health insurance provider, reported a breach of PHI due to an advanced persistent threat attack, an undetected, continuous, and targeted cyberattack for the apparent purpose of extracting data. The initial breach occurred on

December 2, 2014, as a result of a spear phishing email sent to an Anthem subsidiary after at least one employee responded to the malicious email and opened the door to further attacks. This led to the largest U.S. health data breach in history and exposed the electronic protected health information of almost 79 million people. This breach is responsible for the spike visible in Figure 2 above for 2015. "Anthem failed to conduct an enterprise-wide risk analysis, had insufficient procedures to regularly review information system activity, failed to identify and respond to suspected or known security incidents, and failed to implement adequate minimum access controls to prevent the cyber-attackers from Accessing sensitive ePHI." In addition to the $16 million settlement, Anthem was ordered to undertake a robust corrective action plan to comply with the HIPAA Rules.

Discussion: advancing health it in the time of growing threats

The changing priorities highlighted in the 2024–2030 Federal Health IT Strategic Plan reflect the next step in healthcare digitalization. It emphasizes expanding the use of electronic health information, improving interoperability, and advancing automation through AI-based technologies. However, findings from this study, drawing from HHS breach reports, reveal persistent and widening gaps between strategic ambitions and on-the-ground realities. While health IT modernization reduces inefficiencies associated with paper-based systems (storage, handling, and theft of paper records), it simultaneously creates new vulnerabilities in the collection, transmission, and storage of PHI. These findings point to four interconnected areas of tension shaping the digital transformation of U.S. healthcare: (1) the changing origins of threats, (2) the growing scope and scale of PHI breaches, (3) shifting burdens and responsibilities for PHI protection, (4) expanding technological complexity and third-party risk, and (5) the widening digital divide.

1. Changing origins of threats

Between 2013 and 2023, reported breaches increased from 177 in 2013 to 454 in 2023 incidents annually. Over this period, internal threats, such as employee misuse, accidental disclosure, or improper disposal, decreased from 55.4% in 2013 to 20% in 2023 as a proportion of the reported incidents annually. External threats surged from 44.6% in 2023 to 80% in 2023. Cyberattacks increased even more sharply, from 15.3% in 2013 to 79.2% in 2023, as non-cyber incidents (e.g., lost or stolen paper records) steadily decreased from 84.7% in 2013 to 20.8% in 2023. This shift reflects the deepening integration of healthcare systems with digital infrastructures, cloud-based storage, and third-party services. As providers increasingly rely on electronic systems and consumer-facing applications, the attack surface expands, exposing health organizations to sophisticated cybercrime and data exfiltration from around the world. These changing threat origins underscore the need to embed security-by-design principles into every layer of the health IT ecosystem rather than relying on post-hoc regulatory enforcement.

2. Growing scope and scale of breaches

The dataset analysis shows not only an increase in the number of breaches but also their reach and impact. Breaches affecting hundreds of thousands or even millions of individuals have become common. For instance, the 2015 Anthem breach affected nearly 79 million individuals and resulted in a $16 million settlement. In 2018, Ponemon Institute conducted a study sponsored by IBM, "The Cost of a Data Breach," which identified the average cost per stolen healthcare industry record to be $408.00 compared to $148.00 per stolen record of personal or sensitive information from other industries [37]. Even with a greater saturation of stolen PHI records, the U.S. healthcare industry remains an attractive target for cybercriminals globally. The increasing scale of exposure illustrates systemic vulnerabilities: patients' PHI resides in multiple locations, within local networks, third-party servers, and cloud systems, each representing a potential breach vector. Once data is exfiltrated, especially to foreign entities or the dark web, recovery becomes nearly impossible. These findings highlight the structural risks of health data commodification and the limits of reactive remediation strategies.

3. Shifting burdens and responsibilities

When breaches occur, affected individuals bear disproportionate responsibility for mitigation. Standard remedies such as credit monitoring, fraud alerts, or recommendations to monitor accounts, shift the burden of protection from institutions to patients. Meanwhile, covered entities focus primarily on future prevention rather than addressing immediate harms. Even when entities comply with HIPAAs breach notification requirements, providing individual notices, media announcements, and reports to HHS, the information disclosed is typically insufficient to fully assess the scope of the breach or its consequences. Furthermore, organizations that cease operations after a breach often escape accountability, leaving patients without recourse. These findings expose asymmetries in how responsibility is distributed and underscore the need for a more patient-centered model of cybersecurity governance [35].

4. Expanding technological complexity and third-party risk

Further efforts to integrate Patient-Generated Health Data (PGHD) produced through the use of consumer technologies (clinical measurements and observations of daily life) into a clinical setting to improve the quality of care contribute to the complexity of managing PHI [38]. Such technologies include wearable devices, healthcare medical devices, and software health products. The growing use of biomedical technologies both by consumers and providers of health care, along with the effort to integrate and streamline the exchange of data, creates new opportunities for PHI theft and introduces new vulnerabilities that can be exploited regardless of the user's physical location [39]. This growing complexity can be overwhelming to both providers and patients whose PHI was not secured properly.

Starting in late 2022, breaches involving third-party vendors and third-party technologies started to emerge. The incidents involving tracking technologies embedded in hospital websites (e.g., Novant Health and Community Health Network, 2022–2023) show how routine digital marketing tools can lead to impermissible disclosures of PHI to third parties such as Meta and Google. These breaches demonstrate that even nonclinical technologies embedded within healthcare platforms can compromise patient privacy. Third-party relationships thus represent a critical governance blind spot. Although business associates account for nearly 30% of all reported breaches, regulatory frameworks remain fragmented, and enforcement mechanisms are insufficiently coordinated across sectors.

5. The digital divide and health data literacy

Digital health literacy becomes an essential skill in understanding and mitigating cyber-based breached of PHI. Digital health literacy is "the ability to search, find, understand, and evaluate health information from electronic sources and then apply that knowledge to address a health problem" [40]. The growing digital divide [41] between patients and providers of healthcare can become a barrier to quality patient-centric cybersecurity [35], especially with the consideration of the PGHD and increased integration of consumer-based biomedical technologies. The digital divide can also prevent patients from benefiting fully from digitized healthcare system advances [42]. Patients and providers with limited digital literacy are less equipped to recognize threats such as phishing or malicious downloads. As digitalization accelerates, disparities in literacy and access contribute to unequal exposure to risk. Addressing this divide requires integrating cybersecurity education into health IT policy, provider training, and patient engagement strategies.

The paradox emerging from this study is that the same technologies designed to improve efficiency, quality, and interoperability can simultaneously generate new risks. It is challenging to enforce complete data security of PHI to comply with regulatory compliance requirements while also making the data available to different stakeholders, both patients and providers, who need to be able to access the data. Data security and greater electronic system interoperability seem to contradict, but remain a priority within the U.S. Federal Health IT Strategic Plan 2024–2030. The findings underscore that data security and interoperability are not necessarily mutually exclusive goals but interdependent priorities that must be pursued together.

A comparative perspective further underscores the global relevance of these findings. The European Union's General Data Protection Regulation (GDPR) and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) offer more centralized and comprehensive frameworks for protecting personal data and ensuring accountability among data controllers. For example, GDPR explicitly obligates controllers to "demonstrate GDPR compliance" with broad data-protection principles such as accountability, data minimization and security [43, 44]. PIPEDA similarly mandates that private-sector organizations collecting, using or disclosing personal information (including health-related data) implement safeguards and obtain meaningful consent [44, 45]. By contrast, the United States maintains a fragmented and largely privatized approach to data governance, in which health information protection is divided among multiple federal and state entities and heavily dependent on market actors. This regulatory fragmentation contributes to uneven enforcement, inconsistent standards, and limited patient recourse in the event of a breach. Situating U.S. vulnerabilities within this broader international context highlights the need for more cohesive and coordinated governance mechanisms to safeguard health data integrity and public trust in an increasingly digitalized healthcare environment.

Regulatory frameworks such as the HIPAA Security Rule and Breach Notification Rule establish baseline safeguards but were designed for an earlier technological period. The increasing use of AI, cloud platforms, and cross-border data exchanges calls for coordinated governance mechanisms that go beyond compliance. Industry-led initiatives like the Health Information Sharing and Analysis Center (Health-ISAC) and Medical Device Information Sharing and Analysis Organizations (MedISAO) exemplify coordinative efforts to enhance situational awareness, share threat intelligence, and promote best practices [46, 47]. Expanding such

collaborative cybersecurity networks is essential for improving resilience across healthcare systems and the wider health IT supply chain.

Future research should explore how regulatory frameworks can evolve to address cross-sector data sharing and AI-driven health technologies; how cybersecurity burdens are distributed among providers, patients, and third parties; and how investments in digital health literacy can promote equitable participation in secure health IT ecosystems. In sum, advancing health IT in a time of growing threats requires a shift from reactive compliance to proactive, collective governance, one that views cybersecurity not only as a technical challenge but as a public health and social justice imperative.

Conclusion

This paper highlights the complex interplay between technological advancements and emerging vulnerabilities within the U.S. healthcare system from 2013 to 2023. The analysis of unsecured breaches of PHI mandated by the HITECH Act of 2009 reveals that while the implementation of EHR systems and the transition from paper-based to digital health records has improved the efficiency, accessibility, and coordination of care in some respects, it has also created new burdens of administering health IT and exposed the healthcare sector to new forms of threats emanating from increased interconnection and interaction within the cyberspace. The steady rise in cyber-related breaches underscores how greater interconnectivity and data reliance have expanded the healthcare system's attack surface and administrative burdens. These findings highlight the dual-edged nature of health IT adoption: it serves as both a tool for improvement and a vector for potential exploitation.

By combining quantitative analysis of breach data with qualitative examination of regulatory language and breach narratives, this study demonstrates that vulnerabilities stem not only from external threats but also from fragmented governance, uneven compliance, and varying interpretations of "reasonable and appropriate" safeguards under the HITECH Act. These findings highlight that technological innovation alone does not guarantee security or equity, it must be accompanied by coherent policies, adequate resources, and a strong culture of cybersecurity accountability.

Strengthening the resilience of the U.S. health system requires sustained efforts at multiple levels. Policy reforms should focus on integrating cybersecurity standards, improving data governance, and closing gaps in digital literacy among both patients and providers. Addressing the digital divide, both across and within healthcare organizations, remains essential to ensuring that health IT advances do not exacerbate existing inequalities. As the federal government promotes the integration of AI and automation into health IT, future research should critically assess whether these innovations mitigate or deepen current vulnerabilities. Continuous monitoring of breach trends, coupled with transparent reporting and cross-sector collaboration, will be vital to sustaining public trust in digital health infrastructures.

Acknowledgements
Not applicable.

Author contributions
Nataliya D. Brantly wrote the entire manuscript.

Funding
This work was supported by the Ted and Karyn Hume Center for National Security and Technology (Hume Center) at Virginia Tech.

Data availability
Data used for this research are publicly available via the U.S. HHS Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information.https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Declarations

Ethics approval and consent to participate
Not applicable. No human or animal subjects were involved in the research for this article.

Consent for publication
Not applicable.

Competing interests
The author declares no competing interests.

Received: 31 March 2025 / Accepted: 17 November 2025
Published online: 04 December 2025

ReferenCE's

1. HHS. HHS Finalizes Federal Health IT Strategy to Drive Systemic Improvements in Health and Care | HHS.gov.pdf [Internet]. 2024 [cited 2024 Nov 20]. Available from: https://www.hhs.gov/about/news/2024/09/30/hhs-finalizes-federal-health-it-strategy-drive-systemic-improvements-health-care.html.
2. HHS. 2024–2030 Federal Health IT Strategic Plan. . Internet. 2024 Sept. Available from: https://www.healthit.gov/sites/default/files/page/2024-09/ASTP%202024-2030%20Strategic%20Plan_508.pdf.
3. HHS. To whom does the privacy rule apply and whom will it affect?. [Internet]. 2024 [cited 2024 Nov 20]. Available from: https://privacyruleandresearch.nih.gov/pr_06.asp.
4. HHS. 45 CFR Parts 160 and 164. Guidance Specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals for purposes of the breach notification requirements under section 13402 of Title XIII (Health Information Technology for Economic and Clinical Health Act) of the American recovery and reinvestment Act of 2009 request for information. Federal Register [Internet]. 2009;74. Available from: https://www.govinfo.gov/content/pkg/FR-2009-04-27/pdf/E9-9512.pdf
5. Alder S. What is Considered PHI Under HIPAA? [Internet]. The HIPPA Journal. 2025 [cited 2025 Jan 14]. Available from: https://www.hipaajournal.com/considered-PHI-hipaa/.
6. Marron JA. Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. A Cybersecur Resource Guide. NIST. 2024; NIST Special Publication 800.
7. HHS. Summary of the HIPAA Security Rule [Internet]. U.S. Department of Health and Human ServiCE's. 2024 [cited 2025 Oct 22]. Available from: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

8. Farhud DD, Zokaei S. Ethical issues of artificial intelligence in medicine and healthcare. Iran J Public Heal. 2021;50:i–v.
9. Evans RS. Electronic health records: then, now, and in the future. Yearb Méd Inf. 2016;25:S48–61.
10. America. I of M (U. S). C on Q of HC in. Crossing the quality chasm: a new health system for the 21st century. Washington, D.C: National Academy Press; 2001.
11. Donaldson MS, Corrigan JM, Kohn LT. To err is human: building a safer health system. 1st. Washington, D.C: National Academies Press; 2000.
12. Lorenzoni L, Belloni A, Sassi F. Health-care expenditure and health policy in the USA versus other high-spending OECD countries. Lancet. 2014;384:83–92.
13. Wager E, McGough M, Rakshit S, Amin K, Cox C. How does health spending in the U.S. compare to other countries? [Internet]. Health System Tracker. 2025 [cited 2025 Feb 4]. Available from: https://www.healthsystemtracker.org/chart-collection/health-spending-u-s-compare-countries/#Health.
14. CMS. National health expenditure data: Historical.[Internet]. Centers for Medicare & Medicaid ServiCE's. 2024 [cited 2025 Feb 4]. Available from: https://www.cms.gov/data-research/statistics-trends-and-reports/national-health-expenditure-data/historical.
15. Chaudhry B, Wang J, Shinyi W, Maglione M, Mojica W, Roth E, et al. Systematic review : Impact of health information technology on quality, efficiency, and costs of medical care. Ann of Intern Med. 2006;144:742–52
16. Hillestad R, Bigelow J, Bower A, Girosi F, Meili R, Scoville R, et al. Can Electronic Medical Record Systems Transform Health Care?. Potential Health Benefits, Savings, And Costs. Heal Aff. 2017;24:1103–17
17. Ja K, Dc M, Ce G, Karen D, Rs R, Ft G, et al. Use of Electronic Health Records in U.S. Hospitals. N Engl J Med. 2009;360:1628–38
18. Worzala C. Policy Update: Federal Incentives for the Adoption of Electronic Health Records. J Oncol Pr. 2009;5:262–63
19. CMS. Promoting Interoperability Programs [Internet]. Centers for Medicare & Medicaid ServiCE's 2024 [cited 2025 Feb 5]. Available from: https://www.cms.gov/medicare/regulations-guidance/promoting-interoperability-programs.
20. ASTP. About The ONC Health IT Certification Program [Internet]. Assistant Secretary for Technology Policy 2021 [cited 2025 Feb 5]. Available from: https://www.healthit.gov/topic/certification-ehrs/about-onc-health-it-certification-program.
21. ONC. Students Trained for Health IT Employment through the HITECH Workforce Development Programs [Internet] 2014 [cited 2025 Feb 5]. Available fromhttps://www.healthit.gov/data/quickstats/hitech-workforce-development-programs.
22. Abbott PA, Weinger MB. Health information technology:Fallacies and Sober realities – Redux A homage to Bentzi Karsh and Robert Wears. Appl Ergon. 2020;82:102973
23. Brantly ND. Automating Health: The Promises and Perils of Biomedical Technologies for Diabetes Management. 2023; Available from: https://vtechworks.lib.vt.edu/handle/10919/115054
24. Ommaya AK, Cipriano PF, Hoyt DB, Horvath KA, Tang P, Paz HL, et al. Care-Centered Clinical Documentation in the Digital Environment: Solutions to Alleviate Burnout. NAM Perspect [Internet]. 2018;8:1–13. Available from: https://nam.edu/wp-content/uploads/2018/01/Care-Centered-Clinical-Documentation.pdf
25. Reisman M. EHRs: The Challenge of Making Electronic Data Usable and Interoperable. Pharm & Ther [Internet]. 2017;42:572–75. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC5565131/pdf/ptj4209572.pdf
26. Tutty MA, Carlasare LE, Lloyd S, Sinsky CA. The complex case of EHRs: examining the factors impacting the EHR user experience. J Am Méd Inf Assoc. 2019;26:673–77
27. OCR. Health Information Privacy: Business Associates [Internet]. Office for Civil Rights. U.S. Department of Health and Human ServiCE's 2019 [cited 2025 Feb 11]. Available from:https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.
28. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technol Heal Care. 2016;Preprint:1–10
29. 21st Century Cures Act. Pub. L. No. 114-255. 114th Congress. [Internet]. Available from:https://www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf. Dec 13, 2016.
30. Zayas-Cabán T, White PJ. The national health information technology human factors and ergonomics agenda. Appl Ergon. 2020;86:103109
31. FTC. A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority [Internet]. Federal Trade Commission. 2021 [cited 2025 Feb 12]. Available from:https://www.ftc.gov/about-ftc/mission/enforcement-authority.
32. FTC. Health Breach Notification Rule [Internet]. Federal Trade Commission. 2025 [cited 2025 Feb 12]. Available from:https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule.
33. Condry MW, Quan XI. Digital Health Innovation, Informatics Opportunity, and Challenges. IEEE Eng Manag Rev. 2021;49:81–88
34. Al-Qarni EA. Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies. Int J Adv Comput Sci Appl. 2023;14
35. Brantly A, Brantly ND. Patient-centric cybersecurity. J Cyber Policy. 2020;5:1–20
36. HHS. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. [Internet].HHS Archive. 2025 [cited 2025 Jan 14]. Available from:https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
37. 2018 Cost of a Data Breach Study: Global Overview [Internet]. Ponemon Institute. 2018 July. Available from: https://www.intlxsolutions.com/hubfs/2018_Global_Cost_of_a_Data_Breach_Report.pdf
38. Kawu AA, Hederman L, Doyle J, O'Sullivan D. Patient generated health data and electronic health record integration, governance and socio-technical issues: a narrative review. Inf Med Unlocked. 2023;37:101153
39. Brantly ND. Homefront to Battlefield: Why the U.S. Military Should Care About Biomedical Cybersecurity. The Cyber Def Rev [Internet]. 2021;6:93–110. Available from: https://www.jstor.org/stable/27021378
40. de AC. Digital Health Literacy: A Future Healthy Choice. Int J Mob DeviCE's, Wearable Technol, Flex Electron (IJMDWTFE). 2021;11:1–11
41. van Dijk J. The digital divide. Cambridge, UK: Polity Press; 2020
42. Apathy NC, Holmgren AJ, Adler-Milstein J. A decade post-HITECH: Critical Access hospitals have electronic health records but struggle to keep up with other advanced functions. J Am Méd Inf Assoc. 2021;28:1947–54
43. Wolford B. What is GDPR, the EU's new data protection law? [Internet]. GDPR. EU. 2025 [cited 2025 Oct 24]. Available from:https://gdpr.eu/what-is-gdpr.
44. GLG. International Comparative Legal Guides: Digital Health 2024. James Strode. 2024. Available from:https://www.acc.com/sites/default/files/resource/upload/DH24.pdf. [cited 2025 Oct 24]. Available from, Edition [Internet]. Kuan R, editor
45. Zeineddine S. PIPEDA: Data Protection Law in Canada for Organizations & Mental Health Clinicians [Internet]. Mentalyc. 2025 [cited 2025 Oct 24]. Available from: https://www.mentalyc.com/blog/pipeda-canada-data-privacy-law-health-information.
46. Health-ISAC. About Health-ISAC [Internet]. Health Information Sharing and Analysis Center. 2025 [cited 2025 Mar 31]. Available from:https://health-isac.org/about-h-isac/.
47. MedISAO. Medical Device Cybersecurity [Internet]. MedISAO. 2025 [cited 2025 Mar 31]. Available from: https://www.medisao.com.

Publisher's Note

Nataliya Brantly PhD is an Assistant Professor of global health security and health technology policy in the Government and International Affairs (GIA) Program within the School of Public and International Affairs (SPIA) at Virginia Tech. She received her PhD in the Science and Technology Studies (STS) program and her Master of Public Health degree from Virginia Tech. She is the Deputy Director for Health Technologies with the Tech4Humanity Lab, working to promote social scienCE's research on biomedical technologies impacting human health. She studies complex issues pertaining to electronic health governance, consumer biomedical technology security, and the impact of biomedical technologies on the human condition.