Navigating HIPAA, HITECH, and Financial Risks: Compliance Challenges in Healthcare Cybersecurity

Chelsea Anestal

Muma College of Business, University of South Florida

ISM 6328: Information Security and Risk Management

Dr. Samuel Conn

May 8, 2025

Executive Summary

Project Objective

This project's primary objective is to navigate the various compliance challenges within healthcare cybersecurity as it relates to the HIPAA and HITECH regulations, discuss relevant issues, and present some plausible strategies for organizations to employ.

Scope

This project focuses on the healthcare industry, exploring the challenges organizations face in maintaining compliance with HIPAA and the HITECH Act in the context of cybersecurity.

Approach

Through a literature review on the regulatory requirements, cybersecurity challenges and financial implications, I analyze how regulatory requirements impact the cybersecurity strategies and risk management processes of healthcare organizations.

Key Findings

HIPAA and HITECH lay a robust foundation, but practical gaps remain. Cybersecurity breaches cause patient safety and operational risks. Financial strain from compliance and cybersecurity upgrades affects smaller providers most. Emerging technologies like artificial intelligence (AI) introduce new layers of risk, often unregulated.

Recommendations

A few practical solutions were developed in this investigation: (1) foster cybersecurity as a core healthcare priority, (2) increase small to mid-size healthcare provider support, (3) oversight and accountability for EHR and AI vendors, (4) strengthen industry collaboration, and (5) enhance threat intelligence sharing.

Table of Contents

Introduction

The healthcare landscape is undergoing an enormous shift with the introduction of AI-Powered electronic health records (EHR) systems (Batt and Appelbaum, 2025). Even before this, many purported that the system was broken. There was a call for resolution to the amount of time clinicians spent on documentation and concerns on data privacy with the push to EHR adoption. As the landscape continues to undergo various changes, relevant laws such as HIPAA and HITECH are some of the drivers for the continual pursuit of compliant systems that are not only able to support the quadruple aim of healthcare (i.e., improve patient experience, improve population health, reduce cost, and improve provider experiences), but also foster ethical practices, keep data safe, and mitigate bias and other risks.

The HIPAA or Health Insurance Portability and Accountability Act is a federal law that protects privacy and security of individual health information (see Appendix A). It serves as a guide to make it easier for civilians and organizations alike to keep health insurance, keep medical records confidential, and help the healthcare industry reduce administrative costs. The HITECH Act also known as the Health Information Technology for Economic and Clinical Health Act was a law enacted after the HIPAA to strengthen privacy and security rules and promote the adoption of EHR (see Appendix B). This not only worked to support HIPAA, but also added an additional layer to healthcare – technology which in present-day has guided efforts toward interoperability but comes with some key challenges including financial impacts, especially for smaller institutions that may not be able to readily switch to a large-scale EHRs. Though the act does encourage EHR adoption through financial incentives aiming to improve clinical quality measures, there is still an added financial component to adoption including training staff and using organizational change resources (Batt and Appelbaum, 2025). Some

healthcare EHR vendors such as Cerner now called Oracle Health have combated this issue through the Great Plains Health Alliance (GPHA) which was a partnership that allowed them to offer a lower cost community addition of their EHR. However, the financial impact has been a key focus of many discussions of cybersecurity and increased EHR adoption expectations.

Given these challenges, this paper will provide a deeper analysis of the relevant laws and regulations (i.e., HIPAA and HITECH), cybersecurity challenges, and financial impacts. From this analysis, key recommendations will be presented. These recommendations will guide organizations on their approach to compliance and navigate cybersecurity and financial risks.

Literature Review

This literature review explores scholarly and regulatory sources related to HIPAA, HITECH, cybersecurity challenges, and the financial and risk management impacts facing healthcare organizations. It examines the difficulties organizations encounter in maintaining compliance, mitigating cybersecurity risks, and navigating associated financial pressures. Together, these themes establish a foundation for understanding the evolving intersection of healthcare regulation, information security, and organizational resilience.

HIPAA & HITECH Overview

In *Complying with HIPAA and HITECH*, Lincke outlines how HIPAA addresses group health insurance, tax and financial aspects, transaction standardization, and security (Lincke, 2024). Title II of HIPAA regulates the protection of personal health information (PHI) and promotes medical transaction uniformity. Lincke further explains how the 2009 HITECH Act addressed HIPAA implementation gaps. Key security-related provisions include the HIPAA Privacy Rule and Security Rules, as well as the Genetic Information Nondiscrimination Act. A summarized overview of HIPAA and HITECH provisions is included in Appendix A and Appendix B to support the regulatory context of this analysis. While Lincke provides a legal foundation, Lane and Schur examine the tensions between data privacy and research utility.

Lane and Schur, in their article, *Balancing access to health data and privacy: A review of the issues and approaches for the future*, analyze the tension between protecting privacy and enabling access to health data for research (Lane and Schur, 2010). Using a conceptual framework that weighs the risk of de-identification against the utility of shared data, they argue that privacy laws such as HIPAA have, in some instances, lowered the threshold for acceptable risk to a point that restricts data release. Their findings highlight how well-intentioned privacy

protections can inadvertently limit the value of healthcare data, especially in the context of multisource linkage and secondary analysis. Taking this a step further, the HC3 Analysts Note provides details on how privacy regulations impact telehealth.

The HC3 Analysts, in *Securing telehealth: Challenges and solutions*, call attention to the vulnerabilities introduced by integrating technology into healthcare services (HC3, 2025). They emphasize the importance of strong data privacy practices, communication security, and regulatory compliance to mitigate cyber risks in telehealth. The report predicts that advances in technology, standardized protocols, and user education will play a central role in strengthening the security and trustworthiness of telehealth systems. This reinforces the need for structured, proactive approaches to maintaining regulatory compliance as care delivery becomes increasingly virtual.

Alder emphasizes the importance of an incident response plan in meeting the requirements of HIPAA Security Rule (Alder, 2023). A security incident is defined as any attempted or actual unauthorized access, use, or interference with electronic PHI (ePHI). Under the Security Incident Procedures standard, HIPAA-covered entities must implement policies to identify, respond to, mitigate, and document security incidents. Alder outlines the necessary components of a contingency plan, including a data backup plan, disaster recovery procedures, emergency mode operations, regular testing, and workforce protocols. His work highlights that maintaining compliance requires not only technical safeguards but also clearly defined, repeatable processes for emergency response and system recovery.

These sources establish the regulatory foundation essential to understanding how healthcare organizations frame their cybersecurity strategies. The next section explores cybersecurity challenges that arise within the healthcare environment.

Cybersecurity Challenges

In his article, *Effectiveness of cybersecurity regulations*, Sani employs a mixed-methods approach that combines expert interviews and breach report analysis to assess how current regulations impact healthcare organizations (Sani, 2024). His findings indicate that while regulations have improved awareness and encouraged compliance, significant gaps remain in practical implementation – especially among smaller providers. Barriers include limited resources, inadequate training, and general lack of cybersecurity awareness. Sani emphasizes that collaboration and information sharing can help build resilience, and he recommends strengthening existing regulations and promoting best practices. Importantly, he frames cybersecurity not just as a regulatory issue, but as a cultural one, requiring healthcare organizations to adopt proactive mindsets. While Sani outlines the effectiveness of regulations, Alder offers insights from recent breaches that expose persistent vulnerabilities.

In *Lessons from 2024 Healthcare Data Breaches*, Alder highlights how even well-resourced healthcare organizations can fall victim to cyberattacks due to preventable mistakes. He details the Change Healthcare breach, in which a Citrix server lacked multifactor authentication – allowing attackers to use compromised credentials to infiltrate the network. The resulting ransomware attack exfiltrated massive amounts of patient data and caused a service outage that lasted for weeks, affecting patients and providers nationwide. Alder notes that while regulation is important, funding for security upgrades, improved cybersecurity education, and practical guidance are urgently needed. He also calls for reducing administrative burdens, enforcing HIPAA compliance more strictly, and actively addressing the rise of cybercriminal networks. His commentary reflects a growing consensus that compliance alone is insufficient without investment and accountability.

Clarke and Martin, in their article *Managing cybersecurity risk in healthcare*, add a human and organizational perspective to the conversation (Clarke and Martin, 2023). They argue that balancing cybersecurity with usability requires a collaborative approach that includes clinicians, IT professionals, and leadership. Educating end users, involving clinical staff in security planning, and promoting shared ownership are key strategies for maintaining both security and functional patient care systems. Their work underscores that strong cybersecurity depends not just on tools and regulations, but on organizational culture and communication. Finally, Singh et al., in *Cybersecurity in healthcare*, broaden the scope by highlighting the reputational and safety risks of cyber incidents (Singh et al., 2024). They emphasize the need for proactive risk mitigation strategies, including robust risk management frameworks, secure system design, strong encryption protocols, and continuous monitoring. Their analysis reinforces that cybersecurity is not simply a technical problem – it affects the trust, safety, and performance of entire healthcare delivery system.

Together, these perspectives highlight the multidimensional nature of cybersecurity challenges in healthcare. The next section explores how these security issues intersect with financial and risk management concerns.

Financial Impacts & Risk Management

Beauvais et al. evaluate the association between three major EHR vendors – Cerner (Oracle Health), Epic, and Meditech – and hospital financial and quality performance. Their study, which examined 2,667 hospitals, assessed outcomes including net income, Hospital Value-Based Purchasing Total Performance Score (TPS), and subdomains such as efficiency, clinical care, patient experience, and safety. The results showed no statistically significant financial relationship with any vendor. However, Epic was positively associated with higher TPS

outcomes and better patient experience scores, though it was negatively linked to patient safety. Both Oracle Health and Epic were associated with improved efficiency. All three vendors demonstrated modest improvements in clinical care outcomes, though with limited explanatory power. These findings highlight variations in vendor performance that may guide future capital investments, though they also suggest broader systemic issues remain unaddressed.

While Beauvais et al. focus on organizational performance, Narasimhan presents a decentralized approach to improving privacy and operational efficiency in insurance claims (Narasimhan, 2024). In *Enhancing privacy and security in healthcare insurance claims*, he proposes a blockchain-based framework using Hyperledger Fabric to automate data exchange and enforce HIPAA compliance. This system stores patient records, payments, and agreements in an immutable ledger, using smart contracts to streamline claims while safeguarding sensitive data. Performance evaluations showed improvements in both security and processing efficiency compared to traditional systems. Narasimhan's model demonstrates how blockchain can reduce administrative burden and enhance transparency, offering a scalable, privacy-centric solution for a financially strained system.

Building on the concept of systemic impact, Batt and Appelbaum conducted a two-part investigation into the financialization of health IT (Batt and Appelbaum, 2025). In Part I, they argue that while federal incentives successfully promoted EHR adoption, they failed to ensure meaningful improvements in care quality or equitable distribution of financial gains. They document hidden costs – such as staff training, system upgrades, and workflow disruptions – that erode value and contribute to clinician burnout. Despite improved billing and internal communication, the broader net economic effects remain ambiguous, particularly for frontline providers who experience increased documentation burdens and reduced time for patient care.

In Part II, the authors explore how the widespread adoption of EHRs enabled new financial strategies, including layering algorithmic applications and monetizing de-identified patient data. They raise concerns about the lack of independent AI systems oversight, cost shifting practices, and the risks of using biased or inaccurate data for clinical decisions. Companies often use AI recommendations as rigid protocols, shifting liability to care teams without sufficient accountability. They also reveal how HIPAA's de-identification loophole enabled data brokers and marketing agencies to profit from sensitive health information – often without patient awareness.

Their analysis culminates in critique of regulatory gaps and industry shifts. The 2024 Change Healthcare, which exposed one-third of Americans' medical records, illustrates the growing risk tied to centralized health IT vendors. These vendors remain largely unregulated, lacking standardized ways to evaluate system safety or ethical implications. The authors argue that venture capital, private equity, and Big Tech reap financial rewards while healthcare institutions, workers, and patients bear the burden of system failures and cybersecurity threats.

Notable Research Gaps

While the literature discusses regulations and cybersecurity vulnerabilities, significant research gaps remain. Practical solutions for protecting patient privacy, managing costs, and regulating EHR/AI vendors are still underdeveloped. Future research should address these areas to enhance resilience and ethical standards in healthcare cybersecurity.

Relevant Issues

The academic discourse revealed notable gaps which serve as critical issues shaping future opportunities for healthcare cybersecurity and compliance reform. These include:

Patient Privacy: While HIPAA provides foundational protections, growing concerns persist around the use of patient data for commercial purposes. Several questions remain: (1) What constitutes appropriate use of patient data during research and development? (2) When is it ethically acceptable to use de-identified data? (3) Can de-identified data be reliably protected from re-identification? (4) How do emerging technologies – such as voice-activated tools – pose new risks to patient privacy? These concerns reflect the growing tension between innovation and ethical data use in healthcare.

Financial Burden and Cost of Compliance: Securing healthcare systems requires a range of investments, including: (1) Cybersecurity upgrades, (2) Specialized training and staff, and (3) advanced cybersecurity measures (e.g., encryption, intrusion detection). These factors also create a disproportionate burden for smaller providers.

Lack of Oversight for EHR Vendors: Major vendors of EHR, revenue cycle management (RCM), and AI systems operate with minimal scrutiny. Many are introducing novel technologies that outpace existing regulatory frameworks. There is little clarity around whether they meet required security standards, how they perform post-implementation, and recourse for if systems compromise care or patient safety compromise.

AI System Adoption Risks: AI in clinical decision-making introduces risks, including: (1) bias that can negatively impact diagnoses or treatment plans, (2) flawed or non-representative training data leading to inaccurate recommendations, and (3) lack of transparency in system decision making.

These issues call for strategic, evidence-based responses to ensure that technological innovation does not outpace ethical and regulatory safeguards in healthcare.

Conclusion

As healthcare organizations navigate the intersection of cybersecurity, regulation, and financial management, they must balance innovation with patient safety and data integrity. HIPAA and HITECH provide regulatory guidelines, but evolving threats and financial pressures continue to expose persistent vulnerabilities. To address the key challenges and relevant issues discussed, a few practical strategies are critical.

Practical Solutions

To align cybersecurity practices with regulatory standards and minimize operational disruptions, facilities should prioritize the following approaches:

(1) foster organizational cultures that emphasize cybersecurity as a core healthcare priority, (2) increase financial support and training for small to mid-size healthcare providers, (3) implement oversight and accountability for EHR and AI vendors through reviews and certifications, (4) strengthen industry collaboration, and (5) enhance threat intelligence sharing for a unified defense posture.

As the healthcare industry continues to digitize, proactive risk management will remain essential to protecting both patients and institutions. Future initiatives must prioritize ethical data practices, robust cybersecurity infrastructures, and responsible technology adoption to ensure that healthcare innovation advances without compromising safety, privacy, or financial sustainability.

In doing so, healthcare can remain both technologically progressive and ethically grounded – protecting lives and systems security alike.

References

Alder, S. (2023, October 17). HHS stresses importance of having an effective cybersecurity incident response plan. *HIPAA Journal*. https://www.hipaajournal.com/hhs-stressesimportance-of-having-an-effective-cybersecurity-incident-response-plan/

Alder, S. (2025, January 24). Editorial: Lessons from 2024 healthcare data breaches. *HIPAA Journal*. https://www.hipaajournal.com/editorial-lessons-from-2024-healthcare-databreaches/

Batt, R., & Appelbaum, E. (2025, February 11). Financialization through health IT, Part I: Lessons from electronic health systems. *Center for Economic and Policy Research (CEPR)*. https://cepr.net/publications/financialization-through-health-it-part-1/

Batt, R., & Appelbaum, E. (2025, February 11). Financialization through health IT, Part II: From electronic health systems to AI. *Center for Economic and Policy Research (CEPR)*. https://cepr.net/publications/healthcare-financialization-through-information-technology-part-2/

Beauvais, B., Kruse, C. S., Fulton, L., Shanmugam, R., Ramamonjiarivelo, Z., & Brooks, M. (2021). Association of electronic health record vendors with hospital financial and quality performance: Retrospective data analysis. *Journal of Medical Internet Research, 23*(4), e23961. https://doi.org/10.2196/23961

CDC. (2022, February 2). *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. U.S. Department of Health and Human Services. https://www.cdc.gov/phlp/php/resources/health-insurance-portability-andaccountability-act-of-1996-hipaa.html

Clarke, M., & Martin, K. (2024). Managing cybersecurity risk in healthcare settings. *Cureus, 16*(2), e51861. https://doi.org/10.7759/cureus.51861

HC3. (2025, January 8). Securing telehealth: Challenges and solutions [Analyst note]. American Hospital Association. https://www.aha.org/system/files/media/file/2025/01/hc3-analyst note-tlpclear-securingtelehealth-challenges-and-solutions-january-8-2025.pdf

Lane, J., & Schur, C. (2010). Balancing access to health data and privacy: A review of the issues and approaches for the future. *Health Services Research, 45*(5 Pt 2), 1456–1467. https://doi.org/10.1111/j.1475-6773.2010.01141.x

Lincke, S. (2024). Complying with HIPAA and HITECH. In Security Planning and Disaster Recovery (pp. 275–287). Springer. https://doi.org/10.1007/978-3-031-43118-0_19

Narasimhan, L. (2024). Enhancing privacy and security in healthcare insurance claims: A blockchain-based decentralized framework for HIPAA compliance. *International Research Journal of Innovations in Engineering and Technology, 8*(1), 201–208. https://doi.org/10.47001/IRJIET/2024.801025

Sani, M. (2024). Assessing the effectiveness of current cybersecurity regulations and policies for resilience in healthcare data protection. ResearchGate. https://doi.org/10.13140/RG.2.2.30505.20326

Singh, G., Tiwari, D., Goel, P., Vishwakarma, P., Gupta, K., & Verma, A. (2024). Cybersecurity in healthcare: Securing patient health information (PHI), HIPAA compliance framework, and the responsibilities of healthcare providers. *IEEE Xplore.* https://doi.org/10.1109/ACCESS.2024.10593022

HHS. (2013, January 25). *HITECH Act Enforcement Interim Final Rule*. https://www.hhs.gov/hipaa/for-professionals/special-topics/hitechact-enforcement-interim-final-rule/index.html

Appendices

Appendix A

Summary of HIPAA Documentation

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established national standards to protect individuals' medical records and other personal health information (PHI). Key provisions include:

- Privacy Rule: Establishes standards for the protection of PHI, giving patients' rights over their health information, including rights to examine and obtain a copy of their health records and request corrections (CDC, 2022).
- Security Rule: Sets standards for safeguarding electronic protected health information (ePHI) through administrative, physical, and technical security measures.
- Breach Notification Rule: Requires covered entities and business associates to provide notification following a breach of unsecured PHI.
- Enforcement Rule: Specifies penalties for HIPAA violations and outlines procedures for investigations and hearings.

These regulations form the core compliance framework for healthcare organizations managing sensitive patient information.

Appendix B

Summary of HITECH Act Documentation

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 expanded HIPAA's scope, particularly regarding the adoption of electronic health records (EHRs) and enforcement of security measures. Key elements include:

- EHR Incentive Programs: Provided financial incentives to healthcare providers for the adoption and "meaningful use" of certified EHR technology to improve patient care.
- Breach Notification Enhancement: Strengthened requirements for breach notification and expanded obligations to business associates (HHS, 2013).
- Increased Enforcement and Penalties: Introduced tiered civil monetary penalties based on the level of negligence and expanded the Department of Health and Human Services' (HHS) enforcement authority.
- Promotion of Health IT: Supported the development of a nationwide health information technology infrastructure aimed at improving healthcare quality, safety, and efficiency. HITECH builds upon HIPAA’s foundation, emphasizing accountability and encouraging the integration of advanced health information technologies while reinforcing patient data security.