Assignment 3.1: Compliance Analysis of SEC, HIPAA, and FERPA Cybersecurity Regulations

Joshua A. Wortz

University of San Diego

CSOL-540

Dr. Michelle Moore

07/14/2025

Introduction

In today's threat landscape, cybersecurity compliance is essential for protecting sensitive information and maintaining organizational integrity. Three major regulatory frameworks govern cybersecurity obligations in the United States across distinct sectors: the Securities and Exchange Commission (SEC), the Health Insurance Portability and Accountability Act (HIPAA), and the Family Educational Rights and Privacy Act (FERPA).

Regulatory Overview

The SEC oversees cybersecurity compliance for publicly traded companies, primarily through Regulation S-P and Regulation Systems Compliance and Integrity (SCI). Regulation S-P mandates that financial institutions adopt written policies to safeguard customer data using administrative, technical, and physical controls (Schreider, 2020). Regulation SCI ensures system availability and resiliency for key market functions like trading and surveillance. The SEC's 2023 updates to Regulation S-K now require detailed cybersecurity risk and incident disclosures within Form 10-K and 8-K filings. While the goal is transparency, Gao et al. (2022) caution that such disclosures, when vague or boilerplate, may hinder investor trust and regulatory clarity.

HIPAA governs how healthcare organizations handle electronic protected health information (ePHI). The HIPAA Security Rule mandates administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of ePHI (Mireles & Hobaugh, 2024). Covered entities must conduct risk analyses, implement employee training, and maintain breach response protocols. However, many organizations struggle to maintain compliance due to outdated systems, workforce limitations, or complexity in the rules themselves (Smith & Abbasi,

2024; Jones, 2024). HIPAA also includes breach notification rules enforced by the Office for Civil Rights (OCR).

FERPA protects the privacy of student education records in federally funded institutions. It grants rights to parents and eligible students to inspect and amend records. FERPA requires "reasonable methods" to limit access but does not mandate breach notifications or specify technical controls (Mireles & Hobaugh, 2024). While the Department of Education enforces FERPA, its enforcement mechanisms are less formalized than those under the SEC or HIPAA. Institutions participating in Title IV financial aid programs must also comply with the Gramm-Leach-Bliley Act (GLBA), which mandates cybersecurity programs aligned with standards such as NIST SP 800-171 (Oluomachi et al., 2024).

Comparison and Contrast

All three regulations aim to protect sensitive data, but their approaches to risk management differ. The SEC focuses on transparency and public disclosure, mandating that companies report risks and incidents in a way that informs investors without jeopardizing internal security (Kerr & Solove, 2023). HIPAA emphasizes technical, administrative, and physical safeguards, allowing covered entities to adapt requirements based on their size and resources. FERPA, in contrast, centers on individual rights and administrative policy, without imposing strong technical safeguards or breach reporting obligations.

In terms of enforcement, HIPAA and SEC stand out. The SEC can impose substantial penalties for failing to disclose material cyber risks, as seen in enforcement actions following data breaches and noncompliant disclosure filings (Gao et al., 2022). HIPAA enforcement by the OCR includes audits, corrective action plans, and monetary penalties, even for smaller clinics

(Smith & Abbasi, 2024). FERPA's enforcement is weaker; it lacks a private right of action, and penalties are rare.

FERPA's cybersecurity language is vague compared to HIPAA's technical specificity and the SEC's legal disclosure requirements. This ambiguity often leads to inconsistent application across educational institutions (Oluomachi et al., 2024).

Case Study: Equifax Data Breach (SEC)

A significant example of SEC-related enforcement is the 2017 Equifax data breach, which exposed the personal data of over 147 million individuals. Equifax failed to patch a known vulnerability in its Apache Struts web application, leading to unauthorized access (Schreider, 2020). The breach had massive repercussions, including public outrage, loss of investor confidence, and significant litigation.

In *In re Equifax Securities Litigation*, the court ruled that Equifax's public statements about its cybersecurity posture were misleading. Equifax was found to have violated its disclosure obligations under the Securities Exchange Act. Civil penalties were imposed, and the case underscored the importance of transparent and accurate cybersecurity reporting (Kerr & Solove, 2023).

Better compliance with SEC rules—especially around timely patch management and candid disclosure—could have mitigated the damage. Equifax's internal weaknesses and delayed disclosures amplified the breach's impact.

Critical Analysis

Each of these regulations plays a vital role in its domain, but limitations exist. SEC rules incentivize companies to disclose risks, but often lead to vague or generic disclosures that fail to inform investors or improve security posture (Gao et al., 2022). HIPAA sets strong expectations, yet many providers—especially small or rural clinics—lack the resources or expertise to meet them (Jones, 2024). FERPA lags behind modern cybersecurity needs, with minimal guidance on breach response or technical controls.

Additionally, FERPA and HIPAA both rely on terms like "reasonable" or "addressable," which introduce interpretive flexibility but create compliance uncertainty. For example, organizations may over- or under-implement security measures due to a lack of clear benchmarks (Smith & Abbasi, 2024). The human element further complicates compliance—social engineering, phishing, and weak password practices remain leading causes of breaches, despite compliance on paper (Moncy et al., 2023).

Recommendations:

1. **Modernize FERPA** to include technical safeguards and breach notification requirements.
2. **Enhance regulatory guidance** by aligning all three frameworks more closely with NIST or ISO cybersecurity standards.
3. **Support small organizations** with grant funding and standardized toolkits to implement baseline protections.
4. **Mandate security awareness training** across all regulated industries, addressing the human factor in cybersecurity.

Conclusion

The SEC, HIPAA, and FERPA create sector-specific guardrails for cybersecurity, but their impact depends heavily on organizational capacity, clarity of enforcement, and evolving threats. The Equifax breach illustrates how failure to comply with SEC mandates can cause lasting financial and reputational damage. Meanwhile, HIPAA's detail and FERPA's ambiguity show the need for reform and modernization. A unified, risk-based, and scalable regulatory approach will improve cybersecurity resilience across sectors and support better protection of sensitive data in a digital world.

References

Gao, J., Mitra, S., & Zang, J. (2022). Cybersecurity disclosure and real effects: Evidence from the SEC's cybersecurity disclosure guidance. *Journal of Accounting and Public Policy, 41*(6), 106983. https://doi.org/10.1016/j.jaccpubpol.2022.106983

Jones, A. (2024). *Cybersecurity challenges in healthcare*. Old Dominion University. https://sites.wp.odu.edu/aaronjones/wp-content/uploads/sites/34168/2025/03/Cybersecurity-Challenges-in-Healthcare-Research-Paper.pdf

Kerr, O. S., & Solove, D. J. (2023). *Cybersecurity law: Technology and actors* (Ch. 2). West Academic Publishing.

Mireles, M. S., & Hobaugh, J. L. (2024). *Principles of cybersecurity law* (2nd ed.). West Academic.

Moncy, L., Scholl, M., & Townsend, K. (2023). Social engineering: The human vulnerability in healthcare cybersecurity. *Journal of Healthcare Information Security, 18*(2), 55–66.

Oluomachi, C., et al. (2024). Evaluating the effectiveness of U.S. cybersecurity policies across education, finance, and healthcare. *arXiv preprint*. https://arxiv.org/abs/2404.11473

Schreider, T. (2020). *Building an effective cybersecurity program* (2nd ed.). CRC Press.

Smith, M., & Abbasi, M. (2024). Cybersecurity in healthcare: Securing patient health information under HIPAA. *Journal of Information Security Policy & Practice, 15*(1), 10–24.