The Challenge of HIPAA Implementation in Healthcare

Samuel E Barrionuevo

Trevecca Nazarene University

ITI-4270-01: Information Assurance

Dr. Tabernik

29th February 2024

The Challenge of HIPAA Implementation in Healthcare

In early 2024, Green Ridge Behavioral Health which is in Gaithersburg, Maryland was investigated because of a reported ransomware breach case from early 2019. Conducted by the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR), they found this behavioral healthcare provider guilty of violating HIPAA violations because they failed to provide proper risk analysis data to protect electronic protected health information (ePHI). Because of this violation, Green Ridge Behavioral Health is subject to a financial penalty of $40,000 and an OCR monitored correction plan that will take place over the coming three years to improve risk management, employee training, and third-party arrangements. Not only did they suffer definitive OCR imposed penalties but also suffered reputational business ramifications.

Introduction

For my final presentation, I will be presenting on the challenges that healthcare companies and organizations face when implementing HIPAA regulations. One of the goals of HIPAA is to ensure the security and protection of patient health information. Before explaining the challenges of certain meeting HIPAA requirements, I will first explain in my presentation the rules themselves and the requirements.

HIPAA Rules

The privacy rule is more involved with specific personal information and what is required to be considered PII. Examples range from names, photos, and other various personal identifiable information. Significant record tracking and organization is required to successfully document, integrate, and track this information in a way that complies. The security rule delves into the requirements, recommendations, and sections that are primarily audited when the OCR searches for evidence of compliance. Much of the security pertains to healthcare systems and the ePHI of patients and customers. The breach notification rule section is made to protect individuals by holding companies accountable and protecting patients by requiring the proper reporting in the event of PHI breaches. Reporting is required to affected individuals to the HHS and various media. This additionally is vital to event incident response and mitigating total

impact of cybersecurity breaches. Properly meeting these rules requires a review and understanding of what policies and procedures need to be met to be HIPAA compliant.

HIPAA Requirements

After discussing the applicable rules, I will cover the specific requirements that companies need to meet to be HIPAA compliant. Examples are workforce management processes, security, and information access management. I will additionally discuss the challenges that arise when meeting these requirements to properly protect data. Depending on the size of the organization, different challenges arise when meeting HIPAA standards. Larger organizations can properly secure and protect patient data though they face data security challenges. It can be increasingly challenging for smaller organizations that face resource constraints. Lack of training and awareness, undeveloped incident response and reporting, and third-party compliance are examples of issues that these organizations face. Finding solutions to these constraints is vital for healthcare organizations.

HIPAA Violation Cases

Further included will be examples of recent organizations that failed to meet HIPAA compliance. I will discuss and analyze the cause and consequences of failed audits and advise on how similar organizations can achieve HIPAA compliance. Looking into recent audits and interpretations of HIPAA through cases is invaluable in addressing compliance challenges. Investigating recent violation cases can give many lessons learned when facing cybersecurity challenges. It can give insight into how each applicable rule is judged by the OCR and how cases are investigated against organizations that are victim of exposed data and unauthorized access. A number of these cases will be listed and discussed to further cover the challenges that companies face. In addition to the challenges that can be discussed, further looking into the reputational and financial ramifications of noncompliance adds to the importance and challenge of meeting HIPAA requirements.

Data Security Challenges

Next, I will cover a few of the main data security challenges that are threats to companies holding patient information. These include prevalent cybersecurity threats and vulnerabilities that are actively affecting organizations. I will discuss highly damaging and threatening attacks such as phishing and sophisticated spear-phishing, ransomware, and insider threats that can actively threaten the security of patient data for healthcare organizations. Additionally, in this section I will discuss the challenges of keeping health records and the challenges of data interoperability, integrity, and legacy system security. To close this section, I will talk about the challenge of data storage and transmission. Securing stored and transmitted data is challenging across multiple healthcare systems and organizations. The implementation of certain security solutions such as encryption, access controls, and audits can improve the safety of data. Data security is vital in keeping with HIPAA compliance and covering certain challenges.

After I have addressed the threats to data security, I will talk about ways that healthcare vendors can mitigate and avoid breaches in data security. This is vital in meeting HIPAA as breaches of confidentiality, integrity, and availability of data violate compliance. Security measures include the implementation of integrated platforms, robust security measures such as encryption, secure file transfer protocols, and data backups. Along with these measures, I will address proper risk management policies, employee training, and incident response procedures to mitigate the damage of data breaches. Comprehensive cybersecurity measures are vital in addressing data security challenges. Listed alongside security requirements in HIPAA includes security best-practice measures that can be taken to further protect data that. I will discuss integrating these with security best practices and HIPAA requirements to achieve robust security. Combining these with other comprehensive measures is the solution to properly meeting HIPAA compliance.

Conclusion

As I bring the presentation to a close, I will cover the importance of HIPAA compliance in healthcare companies. I will address the key HIPAA rules that relate to information assurance and their part in compliance. Next, I will talk about a few specific rule requirements that are challenging and how

companies fail to achieve them. Further, I will address the specific cases that I mentioned in the presentation and lessons learned from those cases reinforcing the importance of compliance. Lastly, I will mention the data security challenges and ways that companies can mitigate HIPAA violations.

References

Alder, S. (2024, February 22). HIPAA Violation Cases. HIPAA Journal. https://www.hipaajournal.com/hipaa-violation-cases/

Cook, K. A., & Block, A. (2017, December). Improving Health Care Cybersecurity. Risk Management, 64(11), 14+. https://link.gale.com/apps/doc/A519936033/AONE?u=tel_s_tsla&sid=bookmark-AONE&xid=b0b3ebf3

Staton, A. R., & Kielty, M. (2023). A Lurking Threat: Counselor Practices to Guard Against Cyber Threats. Journal of Mental Health Counseling, 45(1), 20+. https://link.gale.com/apps/doc/A733749736/AONE?u=tel_s_tsla&sid=bookmark-AONE&xid=6f0c64ee

Mohammed, D. (2017). US healthcare industry: Cybersecurity regulatory and compliance issues. Journal of Research in Business, Economics and Management, 9(5), 1771-1776.

Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

For additional information on APA Style formatting, please consult the APA Style Manual, 7th Edition.