BOSTON UNIVERSITY METROPOLITAN COLLEGE

CISO Challenges at Cottage Health:
Implementing Risk Strategies

SUBMITTED TO

George Ballesteros, M.S.

MET CS684S O1 REG

Enterprise Cybersecurity Management

by

Michael Nguyen

6/3/2024

In 2018, the Office for Civil Rights (OCR) at the US Department of Health and Human Services (HHS) concluded a record year in enforcing the Health Insurance Portability and Accountability Act (HIPAA). One of the notable settlements involved Cottage Health, which agreed to pay $3 million and implement a corrective action plan following breaches of unsecured electronic protected health information (ePHI). These breaches exposed sensitive patient data and highlighted significant deficiencies in Cottage Health's risk management practices. To enhance their data security and comply with HIPAA regulations, Cottage Health can employ four primary risk management strategies: avoidance, acceptance, mitigation, and transfer. To address the confidentiality, integrity, and availability (CIA) of information needs of HIPAA, ePHI.

1. *List what you consider the top 5 highest risks* for Cottage Health starting with the greatest risk #1, then #2, etc. (Read #2 below before starting #1)

- *Explain your reasoning and logic in the selection and order of the risks you selected. Be specific relating your risks to the heath care entity in the case study.*

1. Unauthorized Access to ePHI

Reasoning and Logic: Unauthorized access to electronic Protected Health Information (ePHI) represents the highest risk for Cottage Health due to its direct impact on patient privacy and potential for significant legal and financial consequences. The case study highlights two breaches in December of 2013 and another one in December of 2015, where ePHI was accessible via the Internet due to misconfigurations in the security settings. Such breaches expose sensitive patient information, including names, addresses, social security numbers, and medical conditions, to unauthorized individuals, posing severe risks to patient confidentiality and trust.

2. Inadequate Risk Assessment and Management

Reasoning and Logic: The failure to conduct accurate and thorough risk assessments to identify potential vulnerabilities in the system is a critical deficiency. Without a comprehensive understanding of the risks assessment, Cottage Health cannot implement effective security measures. The OCR investigation revealed that Cottage Health did not perform regular risk assessments, which likely contributed to the breaches. This systemic issue increases the likelihood of future breaches and regulatory non-compliance, making it the second-highest risk.

3. Lack of Proper Security Configurations and Controls

Reasoning and Logic: The case study details that Cottage Health had significant lapses in security configurations, such as allowing access to ePHI without requiring a username and password. This reflects a broader issue of insufficient security controls and protocols, which are essential for protecting sensitive data. Proper configuration management is crucial for maintaining the integrity and security of ePHI, and its absence can lead to repeated vulnerabilities and data breaches.

4. Insufficient Employee Training and Awareness

Reasoning and Logic: Effective information security relies heavily on employee awareness and training. The breach caused by an IT response to a troubleshooting ticket indicates a potential gap in staff knowledge and adherence to security protocols. Regular training and awareness programs are vital to ensure that all employees understand and follow best practices for data protection, reducing the risk of human error leading to data breaches.

5. Failure to Implement and Enforce Business Associate Agreements (BAAs)

Reasoning and Logic: The OCR investigation found that Cottage Health failed to obtain a written business associate agreement (BAA) with a contractor that maintained ePHI on its behalf. BAAs are crucial for ensuring that third-party vendors comply with HIPAA regulations and protect ePHI appropriately. Without enforceable agreements, Cottage Health cannot hold its business associates accountable for safeguarding ePHI, leading to potential data exposure and regulatory penalties.

- *IMPORTANT – The case study outlines areas of deficiencies in the protection/handling of PHI. Your selection of risk items is not limited to the information in the case study ahead.*

Risk Strategies Considerations: Confidentiality Integrity Availability (CIA)

1. Regular Risk Assessments and Audits: Conducting periodic evaluations to identify and mitigate potential vulnerabilities.
2. Employee Training and Awareness Programs: Ensuring all staff are trained on data protection best practices and aware of security policies.
3. Business Associate Agreements (BAAs): Establishing and enforcing agreements with third-party vendors to ensure they comply with HIPAA regulations.
4. Incident Response and Management: Developing and maintaining an effective incident response plan to address data breaches promptly and efficiently.
5. Data Backup and Recovery Plans: Ensuring regular data backups and having a recovery plan in place to minimize data loss during a breach or system failure.

Addressing Risk with National Vulnerability Database (NVD)

Avoidance

Risk avoidance involves eliminating risks entirely by not engaging in activities that introduce potential hazards. For Cottage Health, this strategy would entail identifying and discontinuing practices or technologies that pose high risks to ePHI security. For example, if certain legacy systems or software applications are identified as inherently insecure and prone to vulnerabilities, Cottage Health should replace them with more secure, modern solutions. Additionally, the organization could avoid storing highly sensitive patient information on easily accessible cloud-based servers and instead utilize more secure, isolated systems.

By avoiding risky configurations and outdated technologies, Cottage Health can significantly reduce the chances of unauthorized access to ePHI. This proactive approach helps

ensure that patient data remains secure, thus maintaining compliance with HIPAA and avoiding the severe repercussions of data breaches (Hillson & Murray-Webster, 2007).

Acceptance

Risk acceptance involves acknowledging a risk and choosing not to mitigate it, typically because the cost of mitigation is higher than the potential impact. For Cottage Health, certain low-impact risks might be accepted after careful consideration. For instance, minor and infrequent software bugs that do not compromise ePHI security or patient care could be tolerated if the cost of fixing them is disproportionately high.

In this context, acceptance should be used sparingly and only for risks that has been thoroughly evaluated and may be manageable. This approach allows Cottage Health to allocate resources more effectively, focusing on higher-priority risks while tolerating minimal, low-impact issues (Hubbard, 2020).

Mitigation

Risk mitigation involves taking steps to reduce the likelihood or impact of a risk. Cottage Health can implement various measures to mitigate the risks identified in the OCR investigation. Firstly, conducting comprehensive and regular risk assessments is critical. These assessments will help identify the potential vulnerabilities in their systems, enabling their organization to address them proactively.

Improving security configurations is another key mitigation strategy. Ensuring that all cloud-based servers and systems require secure authentication (e.g., usernames and passwords) and regularly updating these settings will help protect ePHI from unauthorized access. Additionally, Cottage Health should implement comprehensive employee training programs to enhance the awareness of data security protocols and reducing the risk of human error.

Periodic technical and non-technical evaluations are also essential to adapt to changing environments and operational conditions. This ongoing vigilance ensures that the security measures remain effective over time and that new risks are promptly identified and managed (Aven, 2015).

Transfer

Risk transfer involves shifting the impact of a risk to a third party, often through insurance or outsourcing. Cottage Health can leverage this strategy by obtaining comprehensive cybersecurity insurance to cover potential financial losses from data breaches. This approach ensures that, in the event of a breach, the financial impact on the organization is mitigated.

Additionally, Cottage Health should establish and enforce robust business associate agreements (BAAs) with all third-party vendors who handle ePHI on their behalf. These agreements must require vendors to comply with HIPAA regulations and implement adequate security measures to protect ePHI. By transferring some of the risks associated with data

handling to trusted third parties, Cottage Health can reduce its overall risk exposure while ensuring that vendors are held accountable for maintaining data security (Lam, 2014).

Conclusion

Implementing these four primary risk managements of strategies—avoidance, acceptance, mitigation, and transfer—should significantly enhance Cottage Health's data security and compliance with HIPAA regulations. By avoiding high-risk practices, accepting minimal and low-impact risks, mitigating significant vulnerabilities, and transferring some risks to third parties, Cottage Health can protect sensitive patient information more effectively. These strategies collectively contribute to a comprehensive risk management approach, ensuring that the organization remains resilient to face an evolving cybersecurity threat.

Bibliography

- Hillson, D., & Murray-Webster, R. (2007). *Understanding and Managing Risk Attitude*. Gower Publishing.
- Hubbard, D. W. (2020). *The Failure of Risk Management: Why It's Broken and How to Fix It*. Wiley.
- Lam, J. (2014). *Enterprise Risk Management: From Incentives to Controls*. Wiley.
- National Institute of Standards and Technology (NIST). (2023). *National Vulnerability Database.* Retrieved from https://nvd.nist.gov
- Office for Civil Rights (OCR). (2018). *OCR Concludes All-Time Record Year for HIPAA Enforcement with $3 Million Cottage Health Settlement. U.S. Department of Health and Human Services.* Retrieved from OCR website.
- Aven, T. (2015). *Risk Analysis*. Wiley.

- Hillson, D., & Murray-Webster, R. (2007). *Understanding and Managing Risk Attitude*. Gower Publishing.
- Hubbard, D. W. (2020). *The Failure of Risk Management: Why It's Broken and How to Fix It*. Wiley.
- Lam, J. (2014). *Enterprise Risk Management: From Incentives to Controls*. Wiley.