Implementing Information Security Policies and HIPAA Compliance at a Small Medical Clinic

Winter, 2025

Eyed Mahdi Al Qarni & Jaime A. Roque Soulette | Advisor: Dr. Luna Wahnon Benayoun | Professor: Dr. Yair Levy, Professor of IS & Cybersecurity

Introduction

The healthcare industry faces stringent requirements for protecting patient information and complying with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (U.S. Department of Health & Human Services (HHS), 2023). Small medical clinics are especially vulnerable to cybersecurity threats like phishing attacks, ransomware, and unauthorized access to patient records due to their limited financial resources and absence of dedicated Information Technology (IT) personnel (Argaw et al., 2021; Verizon, 2024). Maintaining confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) is critical to patient trust and avoiding severe legal and financial penalties. This proposed project specifically addresses cybersecurity challenges identified through an initial assessment of a small medical clinic. This assessment highlighted key vulnerabilities that currently affect the clinic's cybersecurity posture and compliance with HIPAA. Therefore, the objective of this proposed project is to mitigate identified cybersecurity risks by developing effective Information Security Policies (ISPs) tailored specifically to the clinic's operational needs, and by establishing a comprehensive compliance plan to improve its overall regulatory adherence.

Problem & Definition

Small medical clinics face increased cybersecurity threats due to the high value of patient data on the black market, making them attractive targets for cybercriminals (Verizon, 2024). Specifically, smaller healthcare organizations like the one in this project often struggle because they lack adequate financial resources and cybersecurity expertise (Argaw et al., 2021). Without dedicated cybersecurity personnel, the clinic is particularly vulnerable to threats such as phishing attacks, ransomware, and unauthorized data access. One significant issue at the clinic identified in the initial assessment is the lack of clearly defined cybersecurity guidelines and policies tailored to their specific operational environment (HIMSS, 2020). Due to unclear cybersecurity guidelines, employees at the clinic may unknowingly engage in risky behaviors, including weak password management, improper handling of sensitive patient information, and susceptibility to phishing scams. These gaps further result in poor access controls, insufficient data encryption, and inadequate monitoring of cybersecurity activities within the clinic (U.S. Department of Health & Human Services, 2023).

Facts

- **Organizational:** The clinic operates on a limited budget and lacks dedicated cybersecurity personnel. IT duties are handled by administrative staff without proper training, which fails to meet HIPAA's requirement for role-based access controls and contradicts NIST's call for assigned security responsibilities.
- **Cultural:** Staff show low awareness of cybersecurity risks, resist new protocols, and inconsistently follow procedures. This undermines both NIST's "Protect" and "Respond" functions and HIPAA's expectations for workforce security awareness and policy enforcement.
- **Technological:** The use of outdated systems without a defined process for managing device security violates HIPAA's technical safeguards (e.g., access control, audit controls) and falls short of NIST's "Identify" and "Protect" functions.
- **Behavioral:** Frequent risky actions, such as clicking phishing links or mishandling patient data, combined with the absence of regular training, conflict with HIPAA's security awareness and training standards and NIST's emphasis on user behavior in the "Protect" and "Respond" domains.

Project Scope & Goals

This project aims to improve the overall information security practices of a small medical clinic by developing and implementing comprehensive ISPs. These policies will be specifically designed to support the clinic's daily operations while aligning with HIPAA regulatory requirements. The ISPs will cover essential areas such as password management, data handling, and incident response. Rather than asserting absolute compliance, the project emphasizes the development of structured and actionable policies that promote risk reduction, encourage staff accountability, and support long-term adherence to security and privacy standards.

Solutions & Action Plan

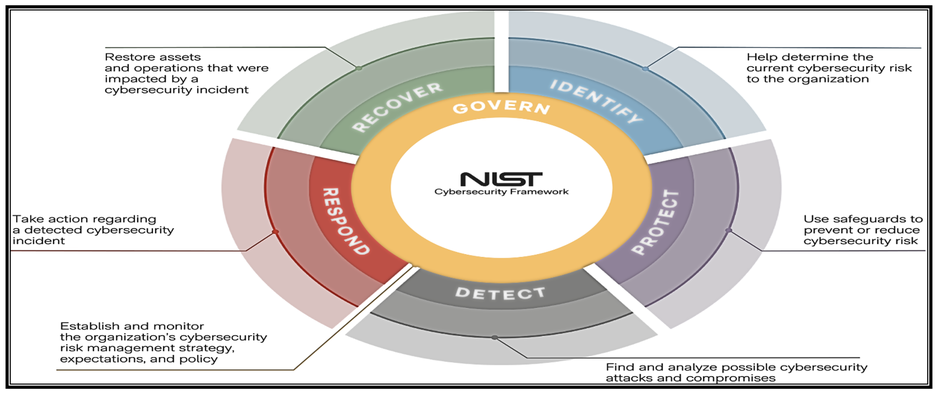

Table 1. Action Plan

ACT#	Action	Responsible Person	Action Type
ACT #1	Develop and implement multiple ISPs (password management, data handling, incident response policies)	Project Team	Managerial
ACT #2	Conduct mandatory cybersecurity raining focused on ISPs compliance	Clinic Manager	Managerial
ACT #3	Conduct regular ISPs compliance audits and cybersecurity reviews	Clinic Manager	Managerial
ACT #4	Implement and enforce strong password management policy	Clinic Manager	Technical
ACT #5	Develop formal incident response policy and conduct practice drills	Project Team	Managerial

Table 2. Risk Management

Rank	Cyber Threat	Risk Statement	Likelihood	Impact	Mitigation Actions (Policies & Compliance)
1	Data breach	Unauthorized access to patient data due to absence of formal ISPs may lead to regulatory penalties and reputational harm.	High	High	Develop and implement clear ISPs outlining password policies, access control, and data management guidelines.
2	Phishing attack	Successful phishing attacks targeting untrained employees may result in unauthorized access to clinic systems and patient data.	High	High	Establish regular mandatory cybersecurity awareness training programs for clinic staff, specifically addressing phishing risks.
3	Data breach	Outdated data handling procedures may lead to improper storage or transmission of patient information, increasing the risk of HIPAA violations.	Medium	High	Develop a clear data handling policy compliant with HIPAA, including encryption requirements and data storage guidelines.
4	Ransomware attack	Delayed incident response to cybersecurity attacks may exacerbate damage and prolong system downtime.	Medium	Medium	Establish a formal incident response policy clearly defining steps for reporting, handling, and reviewing cybersecurity incidents.
5	Malware infection	Failure to conduct regular compliance audits may allow unnoticed vulnerabilities to be exploited by attackers.	Medium	Medium	Implement a structured compliance plan including quarterly audits of policy adherence and security reviews.
6	Unauthorized access	Weak password management practices may lead to unauthorized access to clinic systems and sensitive patient data.	Medium	Medium	Develop and enforce a strong password policy clearly outlining complexity, periodic password changes, and prohibition on password sharing.

Anticipated Results

The implementation of ISPs and supporting compliance measures is expected to improve the clinic's ability to manage security risks and align with HIPAA requirements. By implementing the proposed ISPs and compliance measures, the clinic will strengthen its cybersecurity posture, reduce risks like phishing, data breaches, and ransomware, and enhance protection of ePHI. These improvements will also lower the risk of legal and regulatory penalties. Following the NIST Cybersecurity Framework 2.0 (2024), the clinic is expected to elevate from Tier 1 to Tier 2, reflecting more structured risk management and improved incident response readiness.

Table 3. Costs

Action ID	Item/Action	Responsible Person	Quantity	Total Cost
ACT-1	Develop and implement multiple ISPs (password, data handling, incident response policies)	Project Team	1	$600
ACT-2	Conduct mandatory cybersecurity training focused on ISPs compliance	Clinic Manager	1	$800
ACT-3	Perform policy compliance audits and internal security reviews	Clinic Manager	1	$500
ACT-4	Implement and communicate password management policy	Clinic Manager	1	$400
ACT-5	Develop formal incident response policy and run staff drills	Project Team	1	$600
	Total Estimated Cost			**$2,900**

Conclusion

This project proposes a policy-based approach to address cybersecurity risks identified at a small medical clinic. By ISPs and a structured compliance plan aligned with the NIST Cybersecurity Framework 2.0 (2024), the clinic can take realistic steps to reduce unauthorized access, employee-related errors, and regulatory exposure. The recommendations focused on internal policy development, staff training, incident response, and audits are designed to be achievable with limited resources and contribute to ongoing HIPAA compliance efforts.

References

Argaw, S. T., Bempong, N. E., Eshaya-Chauvin, B., & Flahault, A. (2021). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *Healthcare, 9*(6), 736. https://doi.org/10.3390/healthcare9060736

Healthcare Information and Management Systems Society. (2020). *Cybersecurity in healthcare*. https://gkc.himss.org/resources/cybersecurity-healthcare

IBM Security. (2023). Cost of a data breach report 2023. IBM Corporation. https://www.ibm.com/reports/data-breach

McCumber, J. (1991). *Information systems security: A comprehensive model*. Proceedings of the 14th National Computer Security Conference, National Institute of Standards and Technology.

National Institute of Standards and Technology. (2024). *Framework for improving critical infrastructure cybersecurity (Version 2.0)*. https://www.nist.gov/cyberframework

U.S. Department of Health & Human Services. (2023). *Health information privacy and security*. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

Verizon. (2024). *2024 data breach investigations report*. https://www.verizon.com/business/resources/reports/dbir/