College of Computing and Engineering
NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

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

Eyed Mahdi Al Qarni & Jaime A. Roque Soulette
Assignment No. 4 - Executive Report
Dr. Luna Wahnon Benayoun – Small Medical Clinic
Dr. Yair Levy
ISEC-695-5
Due Date: April 30, 2025

Table of Contents

Executive Summary

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 (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, this proposed project will 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 cybersecurity posture and regulatory adherence.

Problem Identification and 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).

Gather 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 and 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.

Risk Management

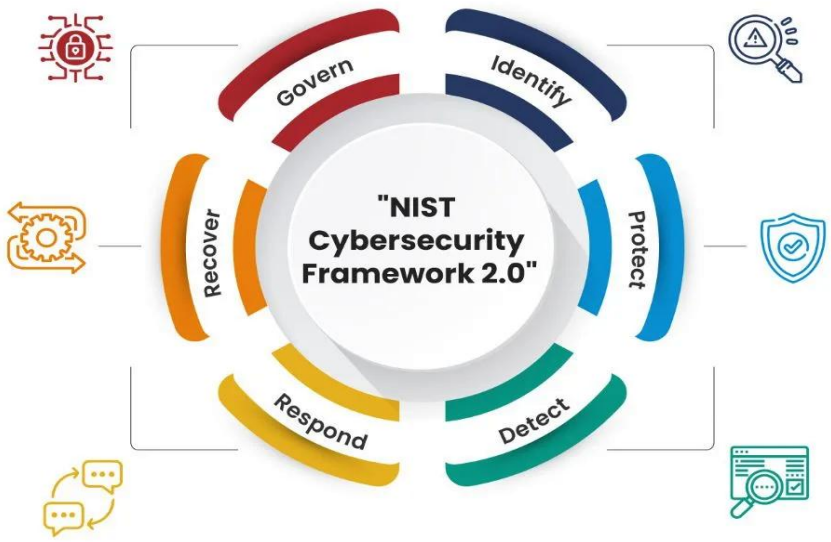
Below is a clearly defined risk management table that identifies and ranks specific cybersecurity risks at the small medical clinic, clearly presenting likelihood, impact, and proposed policy-focused mitigation actions.

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.

Recommended Solution and Action Plan

This proposed project will clearly follow the "**NIST Cybersecurity Framework 2.0 (2024)**" and the "**McCumber Cube Model (McCumber, 1991)**" to mitigate identified cybersecurity risks effectively through clear policies and compliance activities.

Using NIST Cybersecurity Framework 2.0 (2024):



- **Govern:** Establish and maintain organizational cybersecurity risk management policies, roles, and responsibilities to ensure cybersecurity activities align with business objectives and comply with regulatory requirements.
- **Identify:** Conduct regular policy compliance audits to identify areas of non-adherence and vulnerabilities.
- **Protect:** Implement specific cybersecurity policies clearly including password management, secure data handling, and regular employee cybersecurity training.
- **Detect:** Conduct periodic security assessments to detect policy violations or gaps in policy coverage.
- **Respond:** Establish a formal incident response policy clearly outlining immediate actions employees must take during cybersecurity incidents.

- **Recover:** Develop and implement a policy clearly defining procedures for restoring data and services after cybersecurity incidents.

Using McCumber Cube Model (McCumber, 1991):

- **People:** Establish regular cybersecurity awareness training for all clinic employees.
- **Policy:** Develop clear, enforceable ISPs addressing critical cybersecurity areas including password use, secure handling of patient data, and response to cyber incidents.
- **Technology:** Clearly define technology standards for secure data storage and policy enforcement measures, such as secure configuration guidelines.

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

Anticipated Results

By implementing the proposed ISPs and compliance measures, the small medical clinic is expected to significantly enhance its cybersecurity posture. Employees will better understand their responsibilities through structured training and clearer policies, helping reduce the likelihood of errors and non-compliance.

Operational risks such as phishing, data breaches, and ransomware will be mitigated through stronger policies and proactive monitoring. These improvements will also increase protection of ePHI and reduce exposure to legal and regulatory penalties.

Based on the NIST Cybersecurity Framework 2.0 (2024), the clinic currently aligns with Tier 1. Through the implementation of this project, it is anticipated that the organization will elevate to **Tier 2**, indicating partial implementation of defined risk management practices, documented policies, and improved response readiness.

Proposed Costs

The table below shows the estimated costs for carrying out the policy and compliance improvements at the small medical clinic. These costs are based on realistic actions needed to reduce cybersecurity risks and support HIPAA compliance.

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 proposed project addresses critical cybersecurity risks faced by a small medical clinic through the development and implementation of tailored ISPs and a structured compliance plan. These measures focus on improving cybersecurity posture, reducing operational threats, and aligning practices with HIPAA requirements.

Key areas such as phishing risks, employee errors, and inconsistent data handling are addressed through clear policy development, training, and regular compliance audits. Each recommended action aligns with the NIST Cybersecurity Framework 2.0 (2024), which provides a structured approach to strengthening the organization's risk management practices.

In summary, this project provides a realistic, policy-driven roadmap that the clinic can implement within its existing resources to reduce cybersecurity risks and elevate its security practices to industry standards.

Technical Appendix

A. Information Security Policies (ISPs)

1. Password Management Policy

- All system passwords must be a minimum of 12 characters and include a mix of uppercase, lowercase, numbers, and symbols.
- Passwords must be renewed every three months and Reusing any of the previous five passwords is prohibited to enhance account protection.
- Default passwords on all systems must be changed before deployment.
- Staff are prohibited from writing down or sharing passwords under any circumstances.
- Where feasible, MFA should be used to provide an additional layer of security.

2. Data Handling and Storage Policy

- All Patient data should be encrypted when stored and during transfer using NIST-approved encryption standards.
- Portable devices (e.g., USBs, laptops) storing clinic data must be encrypted and authorized by IT.
- Only HIPAA-compliant cloud services are authorized for storing clinic data.
- Staff are restricted from using personal communication tools or devices for handling patient records.

3. Incident Response Policy

- All staff must report suspected or confirmed cybersecurity incidents immediately to the Clinic Manager.

- A designated team will be responsible for logging, assessing, and controlling each cybersecurity incident.
- The clinic will conduct incident response simulations twice per year to assess staff readiness.
- Post-incident reviews will identify root causes and guide policy updates and staff retraining as needed.

B. Compliance Plan

To ensure effective implementation of the above policies and maintain HIPAA compliance, the clinic will adopt the following compliance plan:

- The **Clinic Manager** will be responsible for tracking policy enforcement, reviewing logs, and addressing non-compliance.
- Every three months, internal reviews will evaluate policy compliance and guide updates as needed.
- Cybersecurity policy training sessions will be delivered semi-annually to all staff.
- An annual **third-party compliance review** will be scheduled to assess HIPAA alignment and recommend improvements.
- All policies will be reviewed and revised every 12 months or following a major incident or regulatory change.

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) (NIST Cybersecurity Framework 2.0). National Institute of Standards and Technology.* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

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/

College of Computing and Engineering
NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

Certification of Authorship of Assignment

Submitted to (Professor's Name): **Yair Levy**

Group's Name (Letter): **ISEC-695-5**

Students' Names: **Eyed Mahdi Al Qarni & Jaime A. Roque Soulette**

Date of Assignment: **March 25, 2025**

Title of Assignment: **Implementing Information Security Policies and HIPAA Compliance at a Small Medical Clinic**

Certification of Authorship: By submitting this document we certify that we are the authors of this paper/document/assignment and that any assistance we received in its preparation is fully acknowledged and disclosed in the paper. We have also cited any sources from which we used data, ideas or words, either quoted directly or paraphrased. We also certify that this paper was prepared by us specifically for this course.

We also attest that we have NOT used a generative artificial intelligence (e.g., ChatGPT, Google Bard, Dall-E, Midjourney, etc.) or similar resources on any step of working on this assessment. We are aware that the use of these resources in any way is expressly prohibited and violates the academic standards of NSU and/or a student's academic program as noted in the NSU Student Handbook (p. 15). Additionally, all academic work submitted in this assignment is my original work. I am aware that knowingly giving or allowing my work to be copied, giving out assignment questions or answers, or releasing or selling papers is prohibited. This includes the posting of course content, assignment guidelines, questions and/or answers, or other work submitted for academic credit to online sources or otherwise making such materials publicly available without the prior consent of the professor is an academic misconduct as indicated in the NSU Student Handbook (p. 15).

Students' Signatures ***Eyed Mahdi Al Qarni*** & ***Jaime A. Roque Soulette***