Fall, 2025

Increasing Network-Based Protection against Cybersecurity Threats within a Healthcare Clinic

Student: Jose F Padilla | Business Advisor: Tim Dentes | Professor: Dr. Yair Levy, Professor of IS & Cybersecurity

Introduction

Healthcare clinics utilize electronic Protected Health Information (ePHI) in order to effectively serve patients (Lee, 2022). According to Smith and Abassi (2024), examples of such information include medical histories and billing records. It is clear to see how devastating it would be for such information to fall into the wrong hands. According to Okafor et al. (2023), results could include damaged reputations, financial loss, and exposed patient information. There are many threat vectors from where such devastating attacks can take place. For example, attacks can come from within the business (Alsowail & Al-Shehari, 2021) as well as from outside (Okafor et al., 2023). That is why it is important to implement security controls that help safeguard against cyber attacks. Laws such as the Health Insurance Portability and Accountability Act (HIPAA) have been established to further encourage the protection of ePHI (Yeo & Banfield, 2022). This proposed project will focus on implementing system and network improvements within a dental clinic in order to increase protection against cybersecurity threats.

Problem

Alder (2025) showed that from 2020 to 2025, 4,090 breaches involving 500 or more health records took place in the healthcare industry. Accordingly, around 540,000,000 individuals were affected by the said attacks. Different types of threats include bugs, insiders, phishing, and ransomware, among others (Yeo & Banfield, 2022). Of said breaches, social engineering make up for 78%, insider threats for 17%, theft of devices for 4%, and improper disposal for 1% (Adler, 2025). It is important to describe the previously mentioned attacks to effectively understand the problem. Social engineering is executed by users who attempt to gain access to restricted computers or networks through human manipulation (Cartwright, 2023). Lee (2022) stated that an insider threat are individuals who have or have had access to internal systems and data. That access is then intentionally or unintentionally exploited to cause damage to the business. Devices taken away from office premises are already susceptible to theft. If they are left unencrypted, attackers have an easier time accessing the data within them. Alder (2025) stated that theft of said devices were responsible for a few large data breaches within the last few years. The same author implied that improper disposal could consist of devices that are not wiped clean. Bad actors would find it feasible to access patient data on such devices. The different points of attack shows how it is paramount to have network systems capable of increasing the defense for ePHI. It is also important to understand what technical vulnerabilities could exist to understand the problem well. Technical vulnerabilities consist of weaknesses found within hardware, networks, software, or systems (Lee, 2022). Lee (2022) explained that weaknesses can arise due to poor implementation or lack thereof. Yichen (2020) listed examples that make up said weaknesses. Those include excessive data backups, improper access control, scarce auditing, and shared accounts. Smith and Abassi (2024) listed the lack of transmission with high-encryption measures and unencrypted data as potential weaknesses found within networks. And with clinics having valuable data such as ePHI, the absence of security controls can further encourage attacks from bad actors (Cartwright, 2023).

Gather Facts

The Florida Dental Clinic delivers dental services to those who request it. The small business can align, clean, examine, and replace teeth. The end goal is to improve the customer's health and morale. To accomplish said goal, the business employs six people with overlapping roles. There is one secretary, one technician, three assistants, and the head dentist. All are capable of accessing and managing the software and hardware containing ePHI. The network setup begins with an Arris TG2482 modem situated between the internet and the NetGear GS108 Switch. The modem has firewall capabilities. The switch is connected to two workstations, the encrypted main server, and encrypted backup server through ethernet. It is also connected to three additional workstations, one laptop, three printers, and five cellphones through Wi-Fi. The laptop is connected to a television that runs promotional videos on loop. Throughout the clinic, there is a lack of network segmentation capable of separating devices from interacting with each other. Access control is non-existent, as employees can access all types of data without restriction. There is a Bitdefender Intrusion Prevention System (IPS) installed within each workstation and server. However, the laptop, printers, and cellphones, do not have any prevention or detection system installed. Connection from devices to the server lacks encryption. Employees that have been dismissed are still capable of connecting to the network due to their previous connection to the clinic Wi-Fi. Lastly, logging throughout the clinic is limited to the workstations with Bitdefender installed. The combination of these shortcomings create a large attack vector for would be threat actors.

Project Scope and Goals

The scope of this proposal will focus on enhancing the network security infrastructure currently at the clinic. It focuses on access control, an appropriately placed Intrusion Prevention System (IPS), a cloud backup, device deprovisioning, encryption, network segmentation, and improved logging. The goal of this proposal is to suggest an enhanced network topology capable of mitigating relevant cybersecurity threats to ePHI. Application of National Institute of Standards and Technology (NIST) (2024) standard and the Cybersecurity McCumber Cube (2025) are followed to conform to industry guidelines that help enhance security. The principles brought forth by the organizations are intertwined with the proposed improvements to achieve the goal. For example, improved access control of stored ePHI would come as a result of the application of the Protect function found within the NIST Cybersecurity Framework (CSF) 2.0 (2024). The installation of access control software within the clinic would help in achieving the desired outcome.

Figure 1. NIST Cybersecurity Framework (CSF) 2.0 (2024)

Risk Management

Table 1. Risk Management

Risk Rank	Cyber Threat	Cyber Risk	Likelihood of Occurrence	Impact to Organization	Proposed Action
1	Denial-of-Service	Loss of server access due to successful Denial-of-Service attack	High	High	ACT1
2	Lateral Movement	Gaining unauthorized access to devices by exploiting network segmentation, leading to compromise of ePHI	High	High	ACT2
3	Malware (Trojans, Viruses, Worms)	Loss of sensitive data such as ePHI due to malicious software propagation	Medium	High	ACT3
4	Insider Threat	Manipulation or loss of ePHI due to successful insider threat attack	Medium	High	ACT4
5	Advanced Persistent Threat	Continual loss of ePHI due to covertness from malicious actor found within systems	Low	Medium	ACT5
6	Packet Sniffing	Compromise and loss of ePHI due to exposure of packet data	Low	Medium	ACT6

Recommended Solution and Action Plan

The following recommended solutions and action plans tie into Table 1. For each risk, there is an action plan (ACT) assigned to it. The risk the ACT is assigned to can be identified by their corresponding number. The proposed solution follows the NIST CSF 2.0 (2024) as outlined in Figure 1. The suggested ACT will incorporate the NIST CSF 2.0 (2024) function and category and the Cybersecurity McCumber Cube (2025) security measures. Some ACTs may have multiple proposed actions and NIST CSF 2.0 (2024) Functions.

Table 3. Recommendations

ACT	Cyber Threat	Recommended Solution	NIST Cybersecurity Framework Function	McCumber Cube
1	Denial-of-Service	Implementation of a cloud backup	Protect, Respond, & Recover	Technology
2	Lateral Movement	Network segmentation through virtual local area networks (VLANs)	Protect	Technology
3	Malware (Trojans, Viruses, Worms)	Installation of Intrusion Prevention System (IPS) capable of routing, Wi-Fi, segmentation, and logging	Protect, Detect, & Respond	Technology
3	Malware (Trojans, Viruses, Worms)	Train employees healthy cybersecurity habits	Govern	Awareness, Training, Education
4	Insider Threat	Implementation of Role-Based Access Control (RBAC)	Protect	Technology
4	Insider Threat	Deprovision devices when dismissing employees	Protect	Technology & Awareness, Training, Education
4	Insider Threat	Network segmentation through virtual local area networks (VLANs)	Protect	Technology
5	Advanced Persistent Threat	Installation of device capable of logging, such as an IPS	Protect & Detect	Technology
6	Packet Sniffing	Establishing encrypted network protocols, such as IPsec	Protect	Technology

Proposed Costs

Table 2. Proposed Costs

Equipment/Service Item	Performance By	ACT #	Cost per Item	Number of Items	Total Cost
Microsoft Azure Cloud Backup	Microsoft	1	$30/month	12 months	$360
Initial Setup of Cloud Backup	Independent Contractor	1	$150/hour	4 hours	$600
FortiGate-60F w/ 1 Year Subscription	Fortinet	2, 3, 4, 5, 6	$770	1	$770
Installation of FortiGate-60F	Independent Contractor	2, 3, 4, 5, 6	$150/hour	8 hours	$1,200
Aspire eLearning Training	Aspire eLearning	3	$750	1	$750
Windows Active Directory Setup	Independent Contractor	4	$150/hour	3 hours	$450
Device Deprovisioning Training	Independent Contractor	4	$150/hour	2	$300
Grand Total					**$4,430**

Network Topology

Figure 2. Network Topology - Before

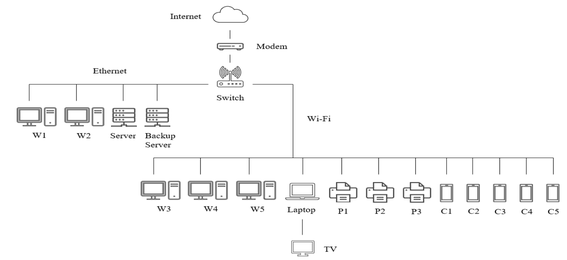
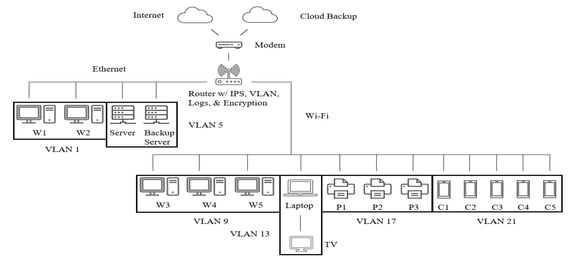


Figure 3. Network Topology - After



Conclusion

This proposal highlights the current state and potential improvements within the network topology of the Florida Dental Clinic. This purpose project seeks to apply solutions to mitigate cybersecurity threats to its ePHI found at the clinic. This proposal focuses on access control, IPS, a cloud backup, device deprovisioning, encryption, network segmentation, and logging. It details the relevant threats introduced by the shortcomings, action plans to mitigate them, and the costs incurred in doing so. The action plans take into consideration the industry accepted frameworks provided by NIST CSF 2.0 (2024) and McCumber Cube (2025) to provide the business with the best possible mitigation under the current circumstances. Application of the suggested actions should increase the NIST CSF 2.0 (2024) tier from where the clinic currently stands, which is Tier 1 (Partial), to Tier 2 (Risk Informed). Tier 1 would indicate that the clinic's ability to manage risks is limited, irregular, and lacking. Tier 2 means that the clinic has improved awareness, consideration, and communication of cybersecurity practices and policies, leading to upgraded risk management. Implementing this proposal help enhance the clinic's network security and provide added protection for its ePHI.

References

Alder, S. (2025, September 30). *Healthcare data breach statistics*. The HIPAA Journal. https://www.hipaajournal.com/healthcare-data-breach-statistics/

Alsowail, R. A., & Al-Shehari, T. (2021). A Multi-Tiered Framework for Insider Threat Prevention. *Electronics*, *10*(9), 1005. https://doi.org/10.3390/electronics1009100

Cartwright, A. J. (2023). The elephant in the room: Cybersecurity in Healthcare. *Journal of Clinical Monitoring and Computing*, *37*(5), 1123–1132. https://doi.org/10.1007/s10877-023-01013-5

Lee, I. (2022). Analysis of Insider Threats in the Healthcare Industry: A Text Mining Approach. *Information*, *13*(9), 404. https://doi.org/10.3390/info13090404

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper No. 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

NCyTE Center. (n.d.). *The McCumber Cube and CIA Triad. NCyTE Center.* Retrieved October 29, 2025, from https://www.ncyte.net/academia/faculty/cybersecurity-curriculum/college-curriculum/interactive-lessons/the-mccumber-cube-and-cia-triad

Okafor, C. M., Kolade, A., Onunka, T., Daraojimba, C., Eyo-Udo, N. L., Onunka, O., & Omotosho, A. (2023). Mitigating cybersecurity risks in the U.S. Healthcare Sector. *International Journal of Research and Scientific Innovation*, *X*(IX), 177–194. https://doi.org/10.51244/ijrsi.2023.10918

Smith, D. A., & Abbasi, N. (2024). Cybersecurity in Healthcare: Securing Patient Health Information (PHI), HIPPA Compliance Framework and the Responsibilities of Healthcare Providers. *Journal of Knowledge Learning and Science Technology*, *3*(3), 278-287. https://doi.org/10.60087/jklst.vol3.n3.p.278-287

Yeo, L. H., & Banfield, J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspectives in Health Information Management*, *19*(2), Article 1i. https://pmc.ncbi.nlm.nih.gov/articles/PMC9123525/

Yichen, Z. (2020). Mitigating Insider Threats in Enterprise Storage Systems: A Security Framework for Data Integrity and Access Control. *International Journal of Trend in Scientific Research and Development (IJTSRD)*, *4*(4), 1878-1890. https://www.ijtsrd.com/papers/ijtsrd31633.pdf