Security Assessment Plan

Office of Information Technology

Simal Sami

April 19, 2023

Contents

1 Introduction

Information security within healthcare is essential to safeguarding both patient and employee data. From 2005 to 2019 the number of individuals impacted by healthcare data breaches was an estimated 250 million and this number only continues to grow as major technological advancements have made it increasingly difficult to ensure total protection of company assets. The procedures within this strategical plan should be closely adhered to not only to ensure security of these assets but also in order to remain in compliance with HIPAA or the Health Insurance Portability and Accountability Act of 1996. This act is a federal law which requires that all protected health information or PHI remain undisclosed unless consented to. PHI is any information included in medical records that can be used to identify an individuals such as name, social security numbers, etc. . Remaining in compliance with HIPAA and employing standard information security practices will allow us to mitigate our risk and protect our assets.

1.1 Purpose

The primary purpose of enacting certain policies, procedures, and security safeguards is to ensure the confidentiality, integrity, and availability of both employee and patient data are retained. This policy and security strategy will serve as a guide to company employees and create certain rules to follow to protect against infringement or unauthorized access. The regulations and restrictions highlighted in this strategy will involve physical safeguards, network infrastructure, employee training, hard-copy medical records, wireless communication, etc.

1.2 Executive Summary

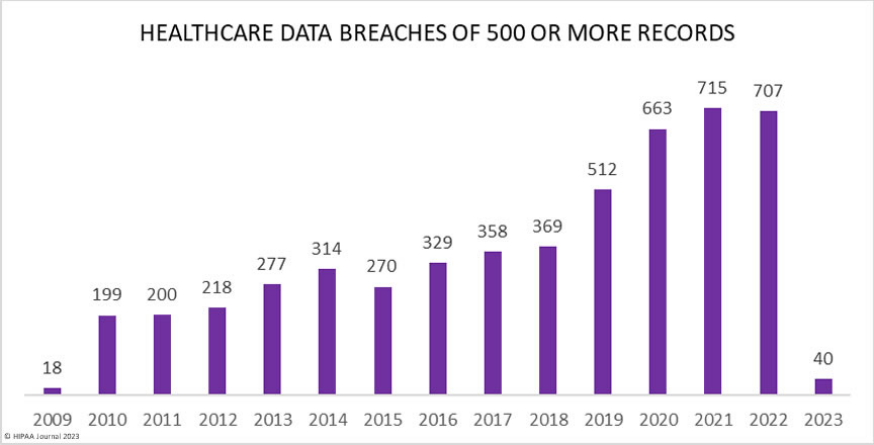


Figure 1: Credit: HIPAA Journal 2023

Security involves everyone and our clinic's mission is to provide quality services that puts patient privacy first. The health sector is a major target for cyberattacks and we must put in all our efforts to protecting our assets. The number of healthcare data breaches have been on the rise since 2001 as depicted in figure 1 and these numbers will only continue to grow. In 2023 so far there have already been 40 major healthcare breaches of at least 500 records of patient information. We are requesting an amount of $250,000 and this budget will allow us to implement security features that can protect our assets and further secure our clinic from falling victim to this statistics. We estimate our security plans will be fully implemented in 7-12 months. We will take both technical and physical precautions to retain the confidentiality, integrity, and availability of our resources and patient data. This includes a tailored network architecture, technical access controls, facility access controls, etc.

2 Identification/Prioritization of Assets and Information

This section works to identify and prioritize our most sensitive assets and goes into detail on how we will handle that information. Information will be classified into two categories: Level 1 and Level 2. These categories will be based on confidentiality, integrity, and availability as well as the harm that would result if the information was exposed. To evaluate confidentiality when

classifying information assets we should look into the impact unauthorized access of that data would have on the clinic and its patients. Integrity should be based upon the level of harm unauthorized modifications to data could potentially have and availability relates to the impact of unreliable access to the asset. We also must take into consideration various other aspects when classifying our assets such as how the information is used, how important it is to day-to-day operations and the cost of repairing damages if the asset is lost. It is crucial to perform reviews of the data and assess their classifications on a timely basis as to ensure they are up to date. These assessments will take place every 6 months and will be conducted by the chief information officer. Any changes to the existing classifications should be communicated to employees within a weeks time and they should take effect immediately. With these levels of classifications in place, we can manage and prioritize our most important assets and ensure that we can allot more of our time and budget into protecting level 2 assets first.

2.1 Level 1

Level 1 assets are often classified as information with can be publicly and readily available to any individual who may seek them out. Breaches of this asset will have little to no impact on daily operations or to the data's integrity, confidentiality, or availability.

2.1.1 Public Website

Our public clinic website will be available online to anyone who may seek it. It will not contain any patient health information but rather information about the facility such as a map, provider directory, etc. If this site were to be breached there would be little disruption to daily operations or loss of crucial data. So we can classify this asset as level 1.

2.2 Level 2

Level 2 assets are those which contain patient health information or other confidential information in which its loss or modification could result in detrimental impacts to the clinic and its HIPAA compliance. The breach of these records should be prioritized and resolved as soon as possible.

2.2.1 Medical Records and Patient Information

Medical records and patient information will be stored in the form of electronic PHI on our online healthcare management platform. A breach of this

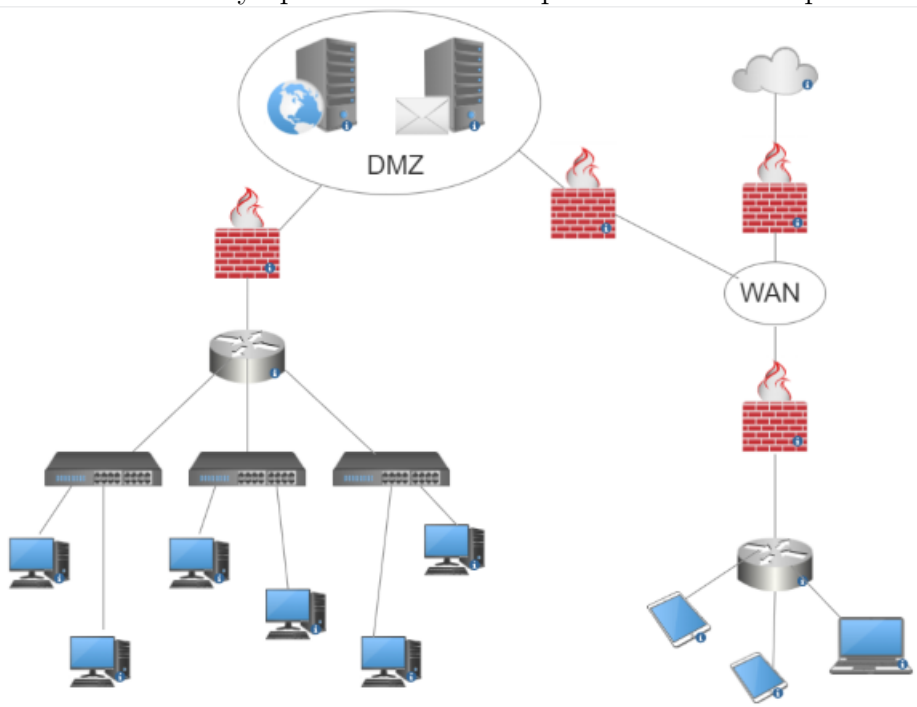
platform could result in a multitude of HIPAA violations and could pose a major threat to our integrity. It is imperative that if PHI is at risk we take steps to remediate the incident and act swiftly.

2.2.2 Billing and Insurance Information

By the end of 2020, data breaches costs healthcare facilities over 6 trillion dollars. Safeguarding insurance and billing information is crucial aspect of information security. Our billing process will take place through an online platform that can ensure the safe storage of this sensitive information.

3 Information System Architecture Design and Topology

Our information system architecture should promote and support communication and ensure daily operations can take place without disruption.



3.1 Network Topology

Network Design considerations are crucial to ensure redundancy and efficiency. We will use a screened subnet architecture with a DMZ and firewalls

to filter external traffic and protect internal traffic. For our firewall rules, all traffic from within the private trusted network will be allowed out but will only be allowed in through exceptions. The web and email servers will within a DMZ to protect between public and private network. We will also use tunnel mode software VPN to encrypt all traffic that is transmitted through an unsecured network. The switches will be each allotted for the reception area, doctors offices, and patient rooms. There will also be a separate wireless network for patients or guests who would like to log on to guest WiFi. An IDS will be implemented within our architecture to prevent and alert us of any threats or possible intrusions.

3.2 Equipment

We will make use of workstation desktops, tablets for patient check ins and laptops for providers. To ensure uniformity, all devices will use windows operating system. There will be about 15 patient rooms each with a desktop machine inside. The reception area will have 3 desktops along with a wired printer to minimize our internet of things devices to reduce cyber-threats. There will also be 3 tablets for patients to fill out appointment forms. We will also have about 15 laptops for distribution amongst providers in the clinic. Telecommunication devices will include analog telephone adapters for faxes and wall/desk phones for both internal and external communication.

4 Defense Methodology

4.1 Technical Safeguards

As technology advances, it becomes increasingly important that we take measures to ensure the protection of our patient health data and records. With the shift from physical health records to electronic health records, technical safeguards will allow of clinic to retain the safety and privacy of our patients.

4.1.1 Access Control

Access control and authorization policies must be followed to ensure we follow a principle of least privilege. Access Control will be managed by the chief information officer who will follow mandatory access control. Employees will only be able to access that data which is necessary to complete ones job. Unnecessary access to patient health records is prohibited. Each user will be assigned a unique ID number which must be used to access patient data or clinic records that are stored electronically. To access a workstation,

one must log in with their assigned identification number and user created password. Additionally, when a workstation is idle for more than 5 minutes, the workstation will automatically log off to ensure no one can access your account. Note that it is crucial to log out off workstations when you leave it.

4.1.2 Audit Control

Audit control will allow us to examine activity that goes on within our information systems that contain ePHI. We will implement a monitoring system that tracks user activity and can create logs. We will store these logs for a minimum of 6 years. Our audits will include user activity within our applications, successful/unsuccessful log ins, and all modifications made by users.

4.1.3 Integrity

Retaining PHI integrity involves making sure unauthorized users cannot destroy or modify health information. To ensure our data is backed up in the event of unexpected downtime or natural disaster we will utilize Google Cloud Service Provider and back our data up to the cloud. It also essential to keep our software updated and install patches in case of vulnerabilities. Once again, our lock out policy and automatic log outs will make sure that no one that is able to access accounts that are not their own.

4.1.4 Authentication

When a person attempts to access patient health information we must ensure that they are who they claim to be. To address this one technique we will implement is a lockout policy. After 10 unsuccessful login attempts, your account will be temporary locked on until you can visit our help desk to verify your identity to unlock it and change your password. Additionally, we will utilize a two-step verification process when logging into our health record system. When setting up their account a user must connect a mobile device to receive a two-step verification notification to when logging in. After entering your username and password, the user will be prompted to send a code to their device which will be required to authenticate their identity.

4.1.5 Transmission Security

Electronically transmitted PHI should be protected from modification or interception by unauthorized individuals in order to retain its integrity. When data is transmitted over an open network such as the internet we will use a VPN which will create a tunnel between the sender and receiver. This

method is both cost-effective and secure. The online platform that we will use for our health portal which stores patient health information will use a secure socket later or SSL certification which will encrypt all data as it passes from the browser through the website server.

4.2 Physical Safeguards

When it comes to security, physical safeguards are just as important as technical safeguards. Securing our equipment and facilities will ensure unauthorized individuals cannot gain entry into areas where important patient data is stored. Physical safeguards act as another line of defense in coordination with technical safeguards. Security officers will be on premise to ensure the safety of our patients, staff, and providers. Any suspicious activity should be reported to them. Our property will also be under 24/7 surveillance.

4.2.1 Facility Access Controls

Facility access controls will allow administrators to ensure that access to facilities is restricted to only those individuals which are authorized to do so. Within out clinic we have various offices, storage rooms, etc which contain either computers or other devices with ePHI or physical copies of PHI. To secure these rooms they are to remained locked and can only be accessed through a card swipe. Each employee will be given an ID card which they must use to swipe into each room. They will be only be able to get into the room if they are assigned authorized entry for that facility. If an employee attempts to swipe into a room in which they are not allowed to access they door will remained locked. We will also log unsuccessful and successful card swipe attempts. It is imperative that employees do not hold the door for individuals behind them. Any filing cabinets that contain confidential patient or billing information must remain locked.

4.2.2 Workstation Use and Security

Workstations or any work-issued laptop or desktop are to be used only for job-related purposes. Browsing the internet or visiting unauthorized sites can increase the risk for data breaches and cyberattacks. As previously mentioned it is important to log out of your account when leaving a workstation. Loss or theft of laptops or other clinic issued devices should be immediately reported to the HIPAA compliance officer as well as the Chief Information Officer. When a device is lost we will access if there was PHI on the device. However, it is advisable that PHI never be stored on devices but only used

to access PHI. It is also important that no unauthorized software is installed on workplace devices.

4.2.3 Device and Media Controls

The use of external devices are prohibited. The use of portable devices increases the risk of malware that can easily be installed on external devices. It also increases the risk of data loss if someone downloads PHI on to the external device and loses it. For employee issued laptops and workplace workstations, the external device capabilities have been disabled.

5 Security Awareness and Training

In order to keep our providers and staff up to date and trained on security protocols, everyone will be required to complete annual Security Awareness Training. The training will provide insight into different types of cyber-threats and how to avoid them. Social engineering attacks ranked as the # 1 attack type in 2022. The training will outline rules for internet and email use along with what not click to avoid falling victim to a phishing attack. It will also educate employees on how to create a secure password. Training is the best way to combat cyberattacks as a result of human error. It will also advise users to report malicious activity to the Chief Information Officer. Security is everyone's responsibility and everyone should be properly trained regardless of their role. All employees regardless of their role will also be required to complete HIPAA training and become HIPAA compliant.

6 Security Incident Procedures and Contingency Plan

Managing threats in real-time can make or break an organization. Setting forth plans in case of emergency can help us be better equipped to deal with security threats or incidents. We will put in place an Incident response plan, disaster recovery plan, and business continuity plan. Incident response plans or IRP will be our immediate response. Incidents are attacks which threaten the confidentiality, integrity, and availability of our information. We will assign the Chief Information Security officer as the incident manager who will be the first point of contact to report an incident to.Firstly, in case the incident results in internet outage we must alert the clinic employees. There should be paper forms available for scheduling appointments and

health forms during the doctor visit. Once the outage is restored this data should be inputted into our electronic system and the physical copies should be shredded. Our various technical safeguard will be our first line of defense in detecting the incidents and figuring out the scale of the attack. We will then categorize the incident on a scale of 1-3, 1 being low, 3 being high based on the level of threat to our clinic. Our preparedness is heavily based on completing security awareness training as well as the technical safeguards we have set in place. This includes malware/anti-virus protection and firewalls. Our physical safeguards will also help to prevent any incidents. We will also ensure our network configuration is redundant and all switch and router configurations are backed up. We want to ensure that all network equipment is on unlimited power supplies that can continue to power equipment without direct power. A disaster recovery plan will help us respond to this incident after they occur. Our plan will help to minimize any interruptions to our everyday operations and help us restore our services in a timely manner. Given our critical role in healthcare and the vast equipment we employ, disaster recovery can be a matter of life or death. We will split our IT staff into teams including the network recovery team, data recovery team.etc. Each team will work to bring back up their sector of IT. We will focus are efforts on bringing up resources which are most important. It is crucial we focus on bringing up our medical equipment first to allow for our daily operations and continue from there. We will look to our backups to replace any compromised data to ensure its integrity.

7 Legal, Compliance, and Public Relation Issues

7.1 HIPAA Compliance Officer

An executive officer will be appointed to be in charge of verifying HIPAA compliance and will be responsibility for handling reports of HIPAA noncompliance and mediating these reports in an appropriate manner. They will also be responsible for reporting breaches of health information that involve more than 500 individuals to the Department of Health and Human Services as well informing impacted individuals of any breaches regardless of its scale. They must help to develop and implement privacy and security policies and stay up to date with new regulations. They may also help conduct workplace HIPAA training and communicate to patients their privacy rights.

7.2 Legal Department

Our clinic will have a legal department to handle legal affairs that relate to HIPAA violations and will help ensure our policies are in line with federal law. They will work closely with the HIPAA compliance officer on matters related to the handling of patient information.

8 Reporting and Metrics

To determine whether our security implementations are effective, it is important to collect various key metrics that can serve as indicators of our performance. The gathering of these metrics will be preformed by the Chief Information Officer along with the HIPAA Compliance Officer. Some statistics we will gather are how many violations of HIPAA were reported in a year. This can reveal how well our training procedures are working to inform employees of the risk of HIPAA breaches and we can implement various changes to our procedures and see what works best to keep our numbers low. Another key metric is the average time in takes for an incident to be reported and then resolved.

9 Staffing

Staffing must fit the needs of the clinic which allows us to give each patient careful attention and an overall good experience. The reception area is crucial as those are the individuals a patient first sees when they walk in the door. The desk must be fully staffed with individuals who can assist with intake forms, scheduling appointments, and office assistants. We will also staff an IT team which can assist with technical needs in the facility. Within this team there will be specialized security technicans who can help employees install and configure required security software as well as hardware. The Clinic's management will consists of a Chief Executive Officer responsible for decision making on behalf of the clinic and maintaining all operations. A Chief Information Officer will be in charge of managing the overall information security program and will develop security plans. The Chief Compliance officer will ensure our policy's and practices are HIPAA compliant while a Chief Financial Officer will take lead on clinic finances and budgeting. We will also employ a Chief Security Officer who will be responsible for the physical aspects of security including monitoring of surveillance footage.

10 Conclusion

Overall, abiding by HIPAA standards will help retain the confidentiality and safety of our patients data. Taking stride to protect this information fulfills our patient's needs effectively and builds a sense of trust. Security is everyone's responsibility and sticking to our technical and physical safeguards will protect confidentiality, integrity, and availability in all aspects of information security.

References

[1] Ge Bai, John (Xuefeng) Jiang, and Renee Flasher. "Hospital Risk of Data Breaches". In: *JAMA Internal Medicine* 177.6 (June 2017), pp. 878–880. ISSN: 2168-6106. DOI: 10.1001/jamainternmed.2017.0336. eprint: https://jamanetwork.com/journals/jamainternalmedicine/articlepdf/2613721/jamainternal_bai_2017_ld_170007.pdf. URL: https://doi.org/10.1001/jamainternmed.2017.0336.

[2] "Health Insurance Portability and accountability act of 1996 (HIPAA)". In: *Centers for Disease Control and Prevention* (2022). URL: https://www.cdc.gov/phlp/publications/topic/hipaa.html.

[3] Adil Hussain Seh et al. "Healthcare data breaches: insights and implications". In: *Healthcare*. Vol. 8. 2. MDPI. 2020, p. 133.