HIPAA & Security

Fernando Mckenzie

(Team Number 00, IT428 System Administration, Bachelor of Information Technology,)

[mckenziegoodenferna@cityuniversity.edu](mailto:mckenziegoodenferna@cityuniversity.edu)

**Abstract**

For the duration of the next ten weeks, team Zero will conduct an Information Security Policy audit based on the security needs of a healthcare organization and potential threats, we will access the healthcare organization within their data systems and review their current protocols. When targeting weak areas, the eight key areas of focus for this executive summary include but it's not limited to information systems Encryption Management, Group Management, Recovery, Restoration & Backup, Network Security, System Hardening, Backup Policy, and Software Development Management policy. Recommendations will also be provided for improvements and implementation of alternative measures to enhance the security of the organization's information systems. Conducting these audits will improve the organization's security footprint and help system administrators to implement effective measures to protect the organization's information systems from potential threats. At the culmination of the ten-week team one’s audit will evaluate the organization’s current policies and procedures in each area and identify any potential weaknesses. Once evaluated, the healthcare organization will begin making changes regarding found vulnerabilities. Overall, our main task is to secure any potential vulnerabilities and inform each respective user of their role within their network. Taking security measures involves them being both internally in the network and externally on the premises. The results of this audit and study will serve as a good reference to those of high-lead roles in a medical environment, or those interested in the technical side. Following these measurements will ensure safety and prevent risk in the future, helping patients and workers simultaneously and effortlessly.

**Keywords:** Data Breach, Network Security, Group Management & Security Rules, RR&B (Restoration, Recovery, and Backup), Encryption Management, System Hardening

**Introduction**

Technology has brought us together in fascinating ways, making it possible to access information wherever we are and using any device. Nonetheless, with these liberties come several major issues, most notably regarding electronically protected health information (EPHI). Electronic protected health information, often known as EPHI, refers to any identifiable health information that is communicated or kept electronically, such as medical records and insurance information. EPHI is safeguarded under HIPAA to ensure that its confidentiality is maintained. To protect the confidentiality of electronically protected health information (EPHI), it is essential for businesses that deal with such data to comply with the requirements established by HIPAA. For businesses to remain in compliance with the HIPAA guidelines, they are required to do frequent risk assessments to determine whether their security policies have any flaws or room for improvement. This contributes to the guarantee that their systems and practices are successful in protecting EPHI and are up to date. It is essential to carry out these evaluations on a regular basis in order to remain one step ahead of any potential threats and to maintain a secure environment for the storage of personal health information.

**Data Breach**

The unlawful acquisition, access, use, or disclosure of protected health information (PHI) that violates the information's security or privacy is what is referred to as a HIPAA data breach. For this section we can discuss the severity of HIPAA non-compliance, and the growth of cyber-attacks and its financial impacts on the healthcare industry from a security standpoint. We will also look at the possible solutions of how to respond before and after a breach occurs, and how to keep proper documentation of processes and procedure. HIPAA mandates PHI handling and storage. Its access, usage, and disclosure. HIPAA compliance helps healthcare providers protect patients' sensitive data, in other words when an organization is non-compliant, they can face steep financial penalties. According to Symplr “Noncompliance with HIPAA may result in fines of up to $50,000 per infraction, regardless of how insignificant they may seem. As to the beginning of 2022, OCR had reached settlements or levied civil monetary penalties totaling $131,392,632 in 106 cases.” (Symplr, 2022).

Critical infrastructure is typically the focus of ransomware attacks, including healthcare facilities, power plants, and government offices. These assaults can create substantial disruption to healthcare organizations, which can result in the loss of access to essential patient health data, hazards to patient safety, and high expenses associated with reacting to and mitigating cyber threats. Researchers in the field of public health examined data from 2016 to 2021 and discovered that the annual number of ransomware assaults increased by more than a factor of two, going from 43 to 91. Out of them, 44.4% caused disturbances in the delivery of healthcare, and 8.6% caused disruptions that lasted for more than two weeks (Fox, 2023). The most common types of disruptions included the malfunctioning of electronic systems, the postponement of scheduled medical appointments, and the redirection of ambulances. In addition, 15.8 percent of ransomware assaults disclosed patient health information, and in some instances, the information that was stolen was made public on the dark web (Fox, 2023).

The HIPAA standards stipulate that the confidentiality of patient information must be always maintained; failing to do so may result in severe penalties.

**What may compliance look like?**

* Reporting Requirements for HIPAA Violations the Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates that covered entities and their business associates notify affected individuals, the Department of Health and Human Services (HHS), and in some instances, the media of any violations of the law that involve the disclosure of personal information. The notification of the breach is to be delivered without an unreasonable delay and no later than sixty days after the breach was discovered at the latest.

**Growth of Healthcare Attacks**

* Many hospitals and clinics were unable to access patient records as a result of the WannaCry ransomware assault, creating delays in treatment and significant dangers to patient safety. Critical medical devices such as MRI machines, which rely on network access to function properly, were also affected by the attack. As a result, visits were canceled, and diagnosis was postponed.
* Noncompliance with HIPAA requirements can have a similar impact. If patient data is not securely secured, fraudsters may gain access to it and use it for harmful purposes such as identity theft or insurance fraud. If the stolen data is utilized to make medical choices, this can result in financial losses, damage to the organization's reputation, and hazards

to patient safety. Furthermore, if a healthcare institution is discovered to be noncompliant with HIPAA standards, it may face hefty fines and legal action, which might jeopardize its financial stability and capacity to offer quality treatment to its patients.

**Network Security**

The process of digitization has had a profound impact on our world. The ways in which we work, learn, play, and live our lives have all evolved. Protecting one's network is an absolute necessity for any company that intends to fulfill the expectations of both its clients and its staff. Network security also helps you safeguard confidential information from being accessed by unauthorized parties. At the end of the day, it safeguards your reputation. The protection of the underlying infrastructure of a network from unwanted access, misuse, or theft is what we mean when we talk about network security (Cisco, 2023). For users, devices, applications, and the infrastructure itself to operate in a secure way, this process requires the creation of a secure infrastructure. The security of a network incorporates several levels of defenses, both at the network's edge and within the network itself. Policies and controls are implemented at each successive layer of the network's security. Users who are authorized to do so are granted access to network resources, while potentially harmful actors are prevented from carrying out exploits and threats (Cisco, 2023). Firewalls, Intrusion Prevention Systems, Virtual Private Networks, and Access Control are some examples of types of network security; however, the list is not exhaustive.

* Firewalls: A firewall is a security device for a network that checks all incoming and outgoing traffic and decides whether to let certain traffic through based on a set of security rules. Firewalls are used to stop people who shouldn't be on a network from getting in.

An intrusion prevention system (IPS) is a piece of software that analyzes network traffic to proactively prevent attacks. Secure intrusion prevention systems achieve this by correlating massive amounts of global threat intelligence to not only stop hostile activity but also track the movement of suspicious files and viruses throughout the network. This aids in the prevention of outbreaks and reinfections.

* The connection from an endpoint to a network can be encrypted via a virtual private network (VPN), which typically operates over the internet. The authentication of the communication that takes place between a device and a network is often handled by either IPsec or Secure Sockets Layer in a remote-access VPN.
* Access Control: You should restrict network access so that not every user can connect to it. You need to be able to identify every person and every device to prevent entry by prospective attackers. After that, you will be able to implement your security policies. You have the option to restrict access for noncompliant endpoint devices or to block them entirely. Control of access to the network is being performed here (NAC).

**Group Management**

The term "user administrator" refers to the process of effectively and efficiently managing user accounts (which are typically associated with software licenses) for the whole of the lifecycles of those accounts in question. Given that licensing measures are based on subscriptions rather than one-time payments, the lifecycle may continue, with licenses being renewed annually or every three years. This is because subscriptions are more cost-effective than one-time purchases. User management, on the other hand, involves making certain that users have the appropriate type of licensing, that they have the appropriate software installed on their device, and, ultimately, that when the user leaves the organization, the license is reclaimed so that it can be distributed to another user.

An organization that controls its users can keep tabs on the number of times a user logs in to pieces of software or data thanks to the capability provided by user management systems (Foxen, 2015).

This information may also be recorded by the organization. User management allows administrators to monitor what users of their program and data can view, how much of it they can see, and whether or not the user has full privileges within the product or the ability to alter any data. In addition, the companies can determine whether the user can alter any data (Foxen, 2015). This helps to improve overall security because it focuses on the 'need to know' basis, and it also has the potential to assist streamline the deployment processes for new software or technologies (Foxen, 2015).

Keeping track of who is authorized to use what inside an organization is a crucial part of being user-based licensing compliant, and effective user management contributes to the openness of user-based licenses. It is crucial to maximize the use of user-based licensing such as Office 365 and Adobe Creative Cloud.

Organizations can save money on software licensing with the help of user management. Knowing how many instances or devices a user has enabled under their license is one way in which an organization may optimize software deployment (Foxen, 2015). If a user requests Office 365 for a mobile device in addition to a laptop, desktop, and phone, the business can see that the customer still has two activations left and doesn't need to purchase a new license.

It is also possible to predict where future software expenditures will be going with the help of user management. Responsible parties can determine which departments (users) inside the company will need certain licenses and when by employing efficient user management (Foxen, 2015). As an added bonus, the company will be able to track when employees no longer need access to specific software, allowing them to repurpose or pool the associated license.

Organizations can benefit from a more proactive approach to the starters, movers, and quitters process when they implement user management (Foxen, 2015). Companies can free up important assets by efficiently managing their users, which guarantees that new users and internal movers experience as little downtime as possible and that a departing employee's hardware and software are returned to IT (Foxen, 2015).

**Security Rules**

The HIPAA Security Rule Standards and Implementation Requirements are divided into four primary areas, each of which was developed to identify pertinent security precautions that contribute to achieving compliance:

1. Needs for the Physical Space

2. Administrative Requirements

3. Technological Requirements

4. Requirements for Policies, Processes, and Documentation

**RR&B**

**(Restoration, Recovery, and Backup)**

**Restoration**

When something goes wrong with your computer, you may use the helpful System Restore feature to roll back to a previous working state. In the event of a catastrophic failure, this can prevent the needless and expensive step of reinstalling or resetting the entire operating system. Restore points are automatically created, but it's still a good idea to generate them on your own every so often.

Confidentiality, integrity, and availability are the three pillars of information security also known as the CIA Triad. When thinking about HIPAA compliance it’s good to keep in mind that servers and computers housing patient information could be damaged in a natural disaster. An organization must review their system and implement a safe method of backup, archiving, and recovery to ensure they are HIPAA compliant (RSI Security, 2022). In the event of a catastrophic data loss, Covered Organizations must have a solid backup plan in place to quickly restore patient records, one example of this is by following the guidelines instructed in CRF 164.308 Administrative Safeguards like section (ii) Implementation Specifications:

1. Risk analysis
2. Risk management
3. Sanction Policy
4. Information System activity review

ECFR. (2023) 45 CFR 164.308(a)(1)(ii)(A)

**Recovery**

Preparation is key to surviving a disaster that could compromise sensitive personal health information (PHI) or interrupt corporate operations and limiting the associated risks. Because of their sudden nature, most disasters catch businesses off guard and leave them unprepared, increasing the likelihood of disruption to their operations. If something happens that isn't in your control and could severely impact your IT infrastructure or compromise sensitive data, we call that a disaster.

For this section It was useful to look at section 7 (i) Standard: contingency plan & (ii) Implementation specifications of CFR164.308. In Section (i) Standard: Contingency plan: Back-up plan, set up policies and procedures for what to do in case of an emergency or other event (like a fire, vandalism, system failure, or natural disaster) that damages systems that hold electronic protected health information (ECFR45 part 164. n.d.). If necessary, put these policies and procedures into action. Section (ii) Implementation specifications:

(A)Data backup plan (Required). Set up and use procedures for making and keeping exact copies of electronic protected health information that can be retrieved.

(B) for dealing with disasters (Required). Set up procedures (and use them as needed) for restoring lost data. Plan for running in emergency mode (Required). Set up procedures (and put them into action as needed) to make sure that critical business processes for protecting the security of electronic protected health information can continue even when the business is in emergency mode.

(D) Procedures for testing and making changes (Addressable). Set up ways to test and change your backup plans on a regular basis.

(E) Analysis of how important applications and data are (Addressable). Assess how important certain applications and data are to other parts of the contingency plan. ECFR (2023) 45 CFR 164.308A(i)&(ii)

ECFR. (2023) 45 CFR 164.308(a)(7)(i)&(ii)

**Backups’**

HIPAA also says that procedures and guidelines for backups must be written down. It's important to make and keep backups according to any written instructions. If a company is ever audited for HIPAA compliance, the auditors will make sure that all backup policies and procedures are well recorded (ECFR45 part 164. n.d.). They will also make sure that backups are done the way the documentation says they should be. If an organization changes how backups are made or how they are kept upto date, it will also have tochange how the procedures are written down (ECFR45 part 164. n.d.).

Data backup is NOT REQUIRED. All Covered Entities (CE), including medical practices and Business Affiliates, must comply with this requirement and ensure that "retrievable exact copies of electronic protected health information" (CFR 164.308(7)(ii)(A)) are securely backed up (ECFR45 part 164. n.d.).

The DATA you are protecting and backing up must be RESTORABLE. (CFR 164.308(7)(ii) (B)) **STORE BACKUP COPIES OF ePHI OFF SITE**. separate from the original data storage. (CFR 164.308(a)(1)) (ECFR45 part 164. n.d.). As a result, your data is present in two physical locations. If something occurs to your office's data, you may immediately retrieve it from distant storage.

Ensure that your data is BACKED UP ON A REGULAR BASIS. The HIPAA Security Final Regulation (CFR 164.308(a)(1)) requires this. The first step in improving Disaster Recovery and Business Continuity is to perform regular backups (HIPAA Security Regulation 164.308(a)(7)(i)).

**Encryption Management**

Encrypting data is an excellent method for preventing unauthorized access to critical information. Every malicious actor can instantly read, access, and use unencrypted data.

Following the compromise of unprotected PHI, the HIPAA's Breach Notification Rule mandates that affected individuals be notified. The word "unsecure" is essential, as the Breach Notification Rule does not apply to material that has been adequately encrypted.

As an illustration, the Athens Orthopedic Clinic agreed to pay $1.5 million to settle various HIPAA violations (WinZip, 2022). This investigation determined that Athens Orthopedic did not utilize data encryption and other security procedures to safeguard patient information.

Following yet another data breach, the University of Rochester Medical Center has paid $3 million to settle charges of HIPAA violations (URMC). Two distinct data breaches involving unencrypted flash drives and computers carrying sensitive patient information led to the settlement (WinZip, 2022)..

Noncompliance with HIPAA requirements increase the likelihood of data loss or theft, even if there is no surefire technique for preventing cyberattacks (WinZip, 2022). Only encryption offers protection against legal disclosure requirements.

HIPAA specifies permissible encryption procedures for data in transit and data at rest to guarantee that PHI is appropriately protected. The HIPAA data at rest encryption standards are consistent with NIST Special Publication 800-111, "Guide to Storage Encryption Systems for End User Devices."(WinZip, 2022).

The following techniques are recommended for encrypting stored PHI:

* application-level encryption (ALE). As ALE encrypts data while it is still in use within an application, the encryption process can be tailored to individual users or groups.
* disk-wide encryption (FDE). FDE modifies the data on a disk drive to render it unreadable. The data on the disk is unavailable without the correct authentication key, even if the hard drive is removed and put in a different device.
* Use of file-level encryption. File-level encryption protects specific files and folders rather than the entire drive. Whole disk encryption provides an additional layer of security because each file is encrypted with a unique key.

**System Hardening**

When hacking a HIPAA server, the underlying deficiency ("exploit") of the software that allows a user to obtain unauthorized access is generally a weakness caused by incorrect configuration or patch application. "Hardening"—also known as "server hardening"—disables system services that are unnecessary, insecure, or both. This is frequently the most crucial component of configuring a protected health information server (PHI) (Trout, 2021).

Several factors determine server hardening. OS. Microsoft Windows and UNIX/Linux variations are popular systems. Windows Servers must stop unnecessary services, install antivirus software, and deploy Windows Updates. Set up security. Windows Server's built-in wizard detects ports/services, configures registry settings, disables unwanted services, and removes firewall rules that don't apply. If a breach occurs, fewer accounts on a production server are safer (Trout, 2021). Windows Server 2008 generates three accounts, including an Administrator. Renaming and disabling this account reduces risk and makes privilege escalation harder if the system is compromised.

Unix/Linux follows the same ideas but implements them differently (Trout, 2021). Disable superfluous services first. The operating system distribution determines how. In Solaris, modifying inetd.conf suffices (Trout, 2021). Some distributions need removing or renaming init files. Blocking the "root" account or logins prevents attackers from gaining superuser access. Properly arranging the /etc/sudoers file can create a complex hierarchy of which accounts can access specific computer files and programs (Trout, 2021).

Web server apps like IIS or Apache should also be hardened (though not all servers are necessarily using a web server application; typically this would only apply to a server that hosts a web portal containing PHI) (Trout, 2021). Doing a simple google search on how to disable modules and functions in IIS and Apache, but this could open the software up to criminal exploitation. These and other resources on server hardening for each platform-type and application and implementation are available online. All HIPAA Vault hosting plans include free server hardening if you don't have time (Trout, 2021).

**Conclusion**

Under the Health Insurance Portability and Accountability Act of 1996, the United States Department of Health and Human Services (HHS) developed a set of federal rules for preserving the privacy of personal health information (HIPAA). This is just a guideline on how to protect patient information and users alike, with proper rights and need to know access. It is good practice to keep up with the latest security trend to help safeguard the public’s information. Going to the HHS Site is a good source of information to help any System Administrator implement a better security plan for all organizations.

**Resources**

Cisco. (2023, January 5). *What is network security?* Cisco. Retrieved March 19, 2023, from https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

ECFR45 part 164. (n.d.). *The Federal Register*. Federal Register :: Request Access. Retrieved March 19, 2023, from https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164#p-164.308(a)(7)(ii)

Fox, A. (2023, January 10). *Half of ransomware attacks have disrupted healthcare delivery, JAMA report finds*. Healthcare IT News. Retrieved March 19, 2023, from https://www.healthcareitnews.com/news/half-ransomware-attacks-have-disrupted-healthcare-delivery-jama-report-finds

Foxen, D. (2015, August 13). *The increased importance of user management*. The ITAM Review. Retrieved March 19, 2023, from <https://itassetmanagement.net/2015/08/13/increased-importance-user-management/>

RSI Security. (2022, October 11). *What is a disaster recovery plan for HIPAA compliance?* RSI Security. Retrieved March 19, 2023, from https://blog.rsisecurity.com/what-is-a-disaster-recovery-plan-for-hipaa-compliance/

Symplr. (2022, March 30). *The financial impacts of compliance missteps*. symplr.com. Retrieved February 18, 2023, from <https://www.symplr.com/blog/financial-impacts-compliance-missteps#:~:text=Costly%20consequences%20of%20HIPAA%20noncompliance,in%20a%20total%20of%20%24131%2C392%2C632>.

Trout, S. (2021, December 28). *Server hardening for HIPAA systems*. Hosting & Cloud Solutions - HIPAA Compliant - HIPAA Vault. Retrieved March 19, 2023, from https://www.hipaavault.com/resources/hipaa-compliant-hosting-insights/server-hardening-for-hipaa-systems/

WinZip. (2022, June 2). How to Comply with HIPAA Data Encryption Requirements. WinZip Enterprise Blog. Retrieved March 19, 2023, from https://winzip.com/blog/enterprise/hipaa-data-encryption-requirements/