HIPAA SECURITY AND PRIVACY COMPLIANCE – A CASE STUDY

Kamana K C, Department of Information Systems, St. Cloud State University, St Cloud, MN 56301, 320-282-7887, kamana.kc6@gmail.com
Jim Chen, Department of Information Systems, St. Cloud State University, St. Cloud, MN 56301 320-308-4882, Jchen@stcloudstate.edu

ABSTRACT

Given the rise in security and privacy breaches in recent years, we think there is still a critical need to improve our understanding of security risks and mitigating measures. Successful defense rests on an in-depth understanding of different policies that govern the use of the information as well as the technologies that can implement such policies. This case study focuses on security and privacy compliance issues in HIPAA and includes a case study about one of the high-profile data breaches that happened back in 2015 and how it's impacted not only the company itself but other businesses as well.

Key Words: **HIPAA Compliance, Data Security, Healthcare Privacy, Anthem**

INTRODUCTION

Most successful organizations today have some sort of web application that their users use to interact with the product and services of the organization. A vast majority of these organizations rely on collecting and using personal information to improve the service to their customers. There are several laws and policies in place that these organizations must follow when collecting critical user information so that if a violation or unauthorized access to the system occurs, the users and their personal information are not adversely affected. Compliance is an industry term that refers to adhering to applicable federal and state laws (Sayles & Gordon, 2020). Security and privacy compliance is an activity that a company or an organization has in place to demonstrate through an audit that they meet the privacy and security requirements that have been established by an external party. Privacy and security compliance is the line between the legal and the illegal. This kind of regulation helps protect customers by ensuring that the company or an organization collecting user data has an appropriate measure in place to handle data appropriately. Failure to comply with the regulations set forth by the external entity results in the company in a certain industry having to pay hefty fines.

History of HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 introduced a security and privacy policy to protect personal health information otherwise known as protected health information (PHI). The HIPAA addresses issues such as health insurance portability after leaving a job, the development of national standards for electronic healthcare transactions, and the creation of national identifiers for providers, health plans, and employers. The HIPAA also addresses health information security and privacy by establishing privacy standards for health information and security standards for electronic health care information. The HIPAA security and privacy compliance rule outlines information such as who is covered under this policy, what information is protected and what measures the

organization in the health industry must take to safeguard protection of electronic protected health information (IPRO, 2022).

The HIPAA act required the Department of Health and Human Services to develop policies and regulations to protect privacy and security of certain health information. To meet this requirement, the HHS published the HIPAA privacy rule which established the national standards for the protection of certain health information. The HHS also published a HIPAA security rule which established a national set of security standards to protect certain health information that is held or transferred in electronic form (HHS, 2022). Prior to the HIPAA security and privacy rule, there were no such policies and regulations in place that would monitor the appropriate use of personal health information. As the internet advanced and the health industry started switching to paperless process of storing health information through online forms, creating such a privacy and security compliance policy was a major importance to protect this information.

Impact of HIPAA on businesses

HIPAA privacy rule does not apply to every person or an organization. It also does not apply to all types of information (HHS, 2022). The privacy rule applies to people or organizations identified as a covered entity (CE), business associates, and workforce. These covered entities must comply with the HIPAA privacy rule. The four types of CE are healthcare providers (hospitals, long-term care facilities, physicians, and pharmacies), health insurance companies, health care clearing houses which processes claims between a healthcare provider and a payer and business associates that includes any person or organization (other than a member of a covered entity's workforce) who uses or discloses individually identifiable health information for the purpose of performing or providing functions, activities, or services for a covered entity (HHS, 2022). In summary, the HIPAA privacy and security compliance policy applies to any health care provider in the health sector who transmits information electronically over the internet. The HIPAA standard ensures the confidentiality, integrity, and availability of all electronic PHI they create, maintain, and transmit. It also identifies any immediate threat to the data and information or the security and the integrity of the systems holding such information. Finally, the HIPAA ensures that all the policies set forth by them are implemented and respected by any provider in the health care industry that transmits user's data electronically over the internet.

In addition, HIPAA addresses many other regulations in place such as privacy and security of health information as well as fraud and abuse. The CE must implement policies and procedures to ensure compliance with the privacy rule. This process includes an ongoing review of privacy policy and procedures and ensuring that all policy changes are consistent with the changes in the privacy and security regulations. Additional legislation has been enacted since its implementation, requiring changes to the HIPAA Rules. The Health Information Technology for Economic and Clinical Health (HITECH) Act, for example, was enacted as part of the American Recovery and Reinvestment Act (ARRA) of 2009. HITECH modifies certain HIPAA Rules provisions to improve patient privacy, security, and enforcement. In addition, HITECH provides economic incentives for healthcare organizations to adopt electronic medical systems in order to reduce healthcare costs (Chen & Benusa, 2017). ARRA/HITECH established tiered penalties, with a range of $100 to $50 000 per violation for unintentional violations. $1 000 to $50 000

per violation if the violation is due to the reasonable cause (known violation with reasonable diligence.) The penalty also includes $10 000 to $50 000 per violation for willful neglect that remained uncorrected. The penalties also set a $1.5 million annual cap for identical violations in each category.

ANTHEM CASE STUDY

Company Background

Anthem, Inc. is a health insurance provider headquartered in the United States. It is the largest for-profit managed health care company in the Blue Cross Blue Shield Association. As of 2018, the company had approximately 40 million members (Anthem Inc., 2018). Anthem is ranked 23rd among the Fortune 500 companies. It was known as WellPoint, Inc. prior to 2014. After both companies acquired several health insurances companies, WellPoint, based in California, and Anthem, based in Indianapolis, merged to form the company in 2004. In California, where it has about 800,000 customers and is the largest health insurer, the company is known as Anthem Blue Cross. In New York, it is known as Empire BlueCross BlueShield, and in ten other states, it is known as Anthem Blue Cross and Blue Shield. Anthem had 45.1 million medical members in October 2021 (Anthem, 2022). The company changed their name to Elevance Health in June 2022. This case study was completed before that so we will be using their former name Anthem Inc.

The Breach

In February 2015, Anthem disclosed a data breach in which cyber attackers gained unauthorized access to one of their parent company's systems. This breach resulted in a compromise of Anthem Blue Cross and Blue Shield employee's information who are now or were previously covered by their health insurance policies or were their consumers. It was the largest single breach of healthcare data in history. The stolen PII (Personally Identifiable Information) included nearly 80 million Americans' social security numbers, medical IDs, birthdates, addresses, and detailed employment and income data; however, no financial or medical information is thought to have been stolen (Shankar & Mohammed, 2020).

Hackers sent phishing emails to an Anthem subsidiary, according to the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR). Phishing is a type of social engineering attack where an attacker poses themselves as a reputable company and sends emails requesting login credentials to a company's database or website. When Anthem's employees receive that phishing email, at least one employee had responded. As a result, attackers were able to install malware on the company's system and used this program to make their way through Anthem's networks, and successfully gained access to more than 50 employee accounts including 90 different systems. The company's data warehouse, which held the records of millions of Anthem members, was one of these systems (HHS, 2022).

Impact and Consequences

As a result of the attack, Anthem was hit with lawsuits and HIPAA non-compliance actions. Anthem has spent $115 million on a class-action lawsuit based on 100 separate cases. The process of notifying the

public of the breach cost more than $30 million. Anthem paid $16 million in HIPAA fines to the Department of Health and Human Services (Young, 2021). Anthem most recently paid a $39.5 million settlement to a group of 44 states in 2020 to settle a variety of breach-related claims. The incident is estimated to have cost Anthem nearly $260 million in total (DeLong, 2014).

LESSONS LEARNED

Organizations can learn various cybersecurity lessons in the aftermath by reviewing the details of this incident, its impact, and Anthem's mistakes along the way. There are a lot of key lessons that companies and users can learn from this incident. Some of the key areas include cybersecurity awareness and training programs, regular monitoring of IT environment, encryption of valuable data and information, implementing and update anti-malware programs and so on (McGee & Ross, 2016).

Companies can have all kinds of complicated and secure technical controls, but these controls will not provide a secure environment if the employees and other users do not understand the importance of securing company's IT environment and their role in maintaining the secure environment. When we talk about IT security and creating a secure environment, the major three controls that needs to be in place are physical controls (camera, locks, ID card access), administrative controls (hiring and termination policies, security awareness training) and technical controls (firewalls, IDS/IPS tools, antivirus). All these controls play a crucial role in a company's overall security and are of equal importance. In Anthem's case, the main reason that the attack was successful was because of the lack of awareness among their employees about cyberattacks. Phishing attack is one of the most common and most popular cyberattack methods. Anthem could have prevented this attack if they had provided proper training to their employees about this attack and how they can protect themselves and company from incidents like this. It is also important to implement a strong password policy and a multi-factor authentication system. This would prevent hackers from getting easy access to the system.

Data encryption must be a top priority in any organization if they are dealing with sensitive and confidential data or information. HIPAA does not make it mandatory for companies to implement encryption. However, in the event of this type of attack, encryption can decrease the impact by huge proportion. Especially in the healthcare industry, leaving data unprotected leads to severe consequences. As we can see in Anthem's case, they did not implement proper data protection protocols leaving their members' records vulnerable and easily accessible. The stolen information can be misused by attackers in many ways like selling in black market, using information to apply for credit cards etc. This incident taught companies and mostly healthcare businesses about the importance of proper encryption of valuable and sensitive data.

CONCLUSION

This study reviewed the history of HIPAA and its impact on current business practices. It also highlighted HIPAA's importance in the healthcare industry as it requires healthcare providers, health plans, healthcare clearinghouses, and HIPAA-covered entities' business associates to implement multiple safeguards to protect sensitive personal and health information. The case study provides a real-life example of how things can go wrong, what lessons learned. While technical controls are necessary, administrative controls such as training, policies and procedures are also important in securing IT infrastructure and data. Future study will investigate preventive solutions for security breaches.

REFERENCES

1. "Anthem: Companies". Retrieved from Anthem Official Website.
2. “Anthem, Inc. 2018 Form 10-K Annual Report". U.S. Securities and Exchange Commission.
3. Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach in History | Guidance Portal (hhs.gov) Retrieved from https://www.hhs.gov/guidance/document/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-us-health-data-breach
4. Chen, J. Q., & Benusa, A. (2017). HIPAA security compliance challenges: The case for small healthcare providers. *International Journal of Healthcare Management*, *10*(2), 135-146.
5. DeLong, J. (2014). “Aligning the Compasses: A Journey through Compliance and Technology”. *IEEE security & privacy*, *12*(4), 85-89.
6. HIPAA and PHI: What Happened After the Anthem Breach - Articles – IPRO Retrieved from https://ipro.com/resources/articles/hipaa-and-phi/#:~:text=Analyzing%20the%20Causes%20this%20HIPAA%20and%20PHI%20ing.
7. McGee, M. K., & Ross, R. (2016, February 26). *Anthem breach: Lessons one year later*. Careers Information Security. Retrieved November 17, 2022, from https://www.careersinfosecurity.asia/anthem-breach-lessons-one-year-later-a-8897
8. Shankar, N. & Mohammed, Z. (2020). Surviving Data Breaches: A Multiple Case Study Analysis. Journal of Comparative International Management, 23(1), 35–54. https://doi.org/10.7202/1071508ar
9. Summary of the HIPAA Security Rule | HHS.gov Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
10. Young, K. (Sept 2021). “Cyber Case Study: Anthem Data Breach” - CoverLink Insurance – Ohio Insurance Agency Retrieved from https://coverlink.com/case-study/anthem-data-breach/