Miray Bolukbasi
Legal Studies
Research Assignment
Prof. Welsh
November 15, 2019

Healthcare Data Privacy

With increasing technology, healthcare institutions have begun to face physical and cyber threats. They are required to protect the personal and health information of their patients. As an example of cyber attacks, we can illustrate the data breach cases. Against these threats, hospitals should establish data protection systems and perform this process under certain laws and rules.

1. Requirements of Healthcare Data Protection

The obligation to protect health data and information by hospitals should be under certain rules, the most important rule that hospital needs to be aware of is "HIPAA".

"Under HIPAA, protected health information is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations (PHI healthcare business uses)."

- There are some entities that supposed to protect health information such as;
- Health plans including health insurance programs, company health plans, and certain government health programs that they pay for health care.
- Health care providers that involved business electronically, and engage with insurance companies electronically, including most doctors, clinics, hospitals, and nursing homes.
- Healthcare clearing houses which process nonstandard health information they receive from another entity into a standard.
- When business associates who are not employees of a covered entity, providing services to covered entity, they need your health information. During that process business associates of covered entities must follow parts of HIPAA regulations (companies that help administer health plans, people like outside lawyers, accountants, and IT specialist).

- The Privacy rule sets rules and limits on who can look at and receive your health information. To make sure that your health information is protected the way that needs to be protected, your information can used and shared:
- For your treatment and care coordinator
- To pay doctors and hospitals for your health care and to help run their businesses
- With your family, relatives, friends, or others you identify who are involved with your health care or your health care bills, unless you object
- To make required reports to police, such as reporting gunshot wounds
- Your health information cannot be used or shared without your written permission unless this law allows it.

2. How This Information is Protected?

Accordingly, U.S. Department of Health and Human Services (HHS), patients' date should be protected but there are some ways to do that. HHS explains that, "covered entities must put in place safeguards to protect your health information and ensure that they do not use or disclose your health information and they must reasonably limit uses and disclosures to the minimum necessary to accomplish their intended purpose". Also, they must have procedures in place to limit who can view and access your health information as well as implementing training programs for employees about how to protect your health information. Business associates must have safeguards to protect patient's information and make sure that they do not use disclose health information improperly.

3. What Are the Violations?

There are most common HIPAA violations by Group One Healthsource website:

- Keeping unsecured records: physical PHI files should be locked, and digital files should require password to access them.
- Unencrypted data: Encrypting the data is an added protection if a device containing PHI is lost or stolen.
- Hacking: It is a real threat to medical ePHI, and there are people out there who want to use this information for malicious purposes, and therefore medical practices need to protect against hacking.

- Loss or theft of devices: If devices containing ePHI are not stored in a secure location at all times, they are subject to the possibly of loss or theft. If the information stored on such devices is not encrypted or password protected, the loss or thief of the devices becomes an even more severe issue.
- Lack of employee training: When it comes to training employees on HIPAA regulations and compliance, it's important that every employee who comes in contact with PHI be thoroughly educated.
- Gossiping- sharing PHI
- Employee dishonesty: When employees try to access PHI that they are not authorized to view, this is a HIPAA violation.
- Improper disposal of records: Educating employees for proper disposal of PHI records is the most important one. Staff members should understand that all healthcare information that contains PHI such as SSN, medical procedures and diagnoses should be shredded, destroyed, wiped from the hard drive.
- Unauthorized release of information: When media members release PHI of public figures or celebrities, it is a violation for HIPAA.
- 3rd party disclosure of PHI: The discussion process should be limited, and the health information should be shared with essential people such as family, doctors or person who is billing for the procedure. If someone has access patient data and share with someone else who do not have right to hear about it, it is a direct violation of HIPAA.

4. How Can Patient Report Violations?

According to HHS, anyone can file a health information privacy or security complaint. The complaint must be filed in writing by mail, fax, e-mail, or via the OCR Complaint Portal. Person who writes the complaint must name the covered entity or business associate involved and describe the acts that believed violated the requirements of Privacy, Security or HIPAA.

Complaint Portal offers patients to complaint about following violations,

"The U.S. Department of Health and Human Services (HHS) and Office for Civil Rights (OCR), enforces federal civil right laws, conscience and religious freedom laws, the Health Insurance Portability and Accountability Act (HIPAA), Privacy, Security and Brach Notification Rules, and the Patient Safety Act and Rule, which together project your fundamental rights of

nondiscrimination, conscience, religious freedom, and health information privacy at covered entities.

- Federal Civil Rights Laws protects unfair treatment because of your differences.
- Federal Conscience and Religious Freedom Laws protect coercion, discrimination on the basis of conscience or religion, and burdens on the free exercise of religion.
- The HIPAA Privacy Rule is a federal law that gives patients' rights over their health information and sets rules and limits on who can look at and receive healthcare information.
- The HIPAA Security Rule is a federal law that requires security for health information in electronic form. In addition, Patient Safety Act and Rule establishes a voluntary reporting system to enhance the data available to assess and resolve patient safety and health care quality issues and provides confidentiality protections for patient safety concerns.

5. What are the consequences of violations?

Since HIPAA requires covered entities to provided training to staff to make sure that HIPAA Rules and regulations are able to be applied. During training, healthcare employees should be aware of the possible penalties for HIPAA violations. There are some consequences that will be faced, if someone breaks HIPAA rules:

- The violation could be dealt with internally by an employer
- Could be terminated, face sanctions from professional boards or face criminal charges which includes fines and imprisonment.

According to HIPAA Journal Website, there are two types of penalties for the HIPAA;

- Civil Penalties: "Civil penalties for HIPAA violations start at $100 per violation by any individual who violates HIPAA Rules. The fine can rise to $25,000 if there have been multiple violations of the same type. These penalties are applied when the individual was aware that HIPAA Rules were being violated or should have been aware had due diligence been exercised. If there was no willful neglect of HIPAA Rules and the violation was corrected within 30 days from when the employee knew that HIPAA Rules had been violated, civil penalties will not apply."
- Criminal Penalties: "The criminal penalties for HIPAA violations can be severe. The minimum fine for willful violations of HIPAA Rules is $50,000. The maximum criminal

penalty for a HIPAA violation by an individual is $250,000. Restitution may also need to be paid to the victims. In addition to the financial penalty, a jail term is likely for a criminal violation of HIPAA Rules.

Also, the consequences always depend of the severity of the violation. OCR prefers to resolve HIPAA violations using non-punitive measures, such as with voluntary compliance or issuing technical guidance to help covered entities address areas of non-compliance, financial penalties may be appropriate. The four categories used for the penalty structure are as follows:

- **Tier 1:** A violation that the covered entity was unaware of and could not have realistically avoided, had a reasonable amount of care had been taken to abide by HIPAA Rules
- **Tier 2:** A violation that the covered entity should have been aware of but could not have avoided even with a reasonable amount of care. (but falling short of willful neglect of HIPAA Rules)
- **Tier 3:** A violation suffered as a direct result of "willful neglect" of HIPAA Rules, in cases where an attempt has been made to correct the violation
- **Tier 4:** A violation of HIPAA Rules constituting willful neglect, where no attempt has been made to correct the violation

In the case of unknown violations, where the covered entity could not have been expected to avoid a data breach, it may seem unreasonable for a covered entities to be issued with a fine. OCR appreciates this and has the discretion to waive a financial penalty. The penalty cannot be waived if the violation involved willful neglect of Privacy, Security and Breach Notification Rules.

6. Reference Case for HIPAA Violation

As a reference, I would like to use Anthem Data breach case, which includes over 78 million of its members stolen healthcare information by cybercriminals. As a violation consequence, Anthem agreed to paid 16 million to Office of Civil Rights. Also, during the investigation that OCR was charge of, they made Anthem to address the compliance issues discovered by OCR.

As an information, Anthem was an independent licensee of the Blue Cross and Blue Shield is America's second largest health insurer. In 2015, cybercriminals had breached Anthem's

defenses and had gained access to its systems and member's sensitive data. As we talk at the beginning of the research, with innovative technology, attackers are able to hack the systems and reach entities' healthcare information. Now, in this case even though Anthem did not purposely give its' health information to criminals, they are still responsible to protect member's information.

With the detailed research, they figured out that attackers first gained access to Anthem's IT systems in 2014. During that time, they stole 78.8 million plan members, including names, addresses, medical identification and their SSNs. The reason that attackers gained a foothold in Anthem's network is they went through spear phishing emails sent to one of its subsidiaries.

The Office of Civil Rights investigation claimed multiple potential violations of HIPAA Rules. The following ones are the violations that Office of Civil Rights sued Anthem for:

- 45 C.F.R. § 164.308(u)(1)(ii)(A) – A failure to conduct a comprehensive, organization-wide risk analysis to identify potential risks to the confidentiality, integrity, and availability of ePHI.
- 45 C.F.R. § 164.308(a)(1)(ii)(D) – The failure to implement regularly review records of information system activity.
- 45 C.F.R. § 164.308 (a)(6)(ii) – Failures relating to the requirement to identify and respond to detections of a security incident leading to a breach.
- 45 C.F.R. § 164.312(a) – The failure to implement sufficient technical policies and procedures for electronic information systems that maintain ePHI and to only allow authorized persons/software programs to access that ePHI.
- 45 C.F.R. § 164.502(a) – The failure to prevent the unauthorized accessing of the ePHI of 78.8 million individuals that was maintained in its data warehouse.

The director of the HHS and OCR, Roger Severino, decided that "Anthem failed to implement appropriate measures for detecting hackers who had gained access to their systems to harvest passwords and steal people's private information". In addition to money that Anthem paid to OCR, they were also liable to pay 19.1 million dollars to their customers whose sensitive information was stolen. As a result, Anthem agreed to settle the lawsuit of 115 million. *($16 Million Anthem HIPAA Breach Settlement Takes OCR HIPAA Penalties Past $100 Million Mark. (2018, October 16).)*

The Works Cited

$16 Million Anthem HIPAA Breach Settlement Takes OCR HIPAA Penalties Past $100 Million Mark. (2018, October 16). Retrieved from https://www.hipaajournal.com/16-million-anthem-hipaa-breach-settlement-takes-ocr-hipaa-penalties-past-100-million-mark/.

HHS Office of the Secretary,Office for Civil Rights, & Ocr. (2017, February 1). Your Rights Under HIPAA. Retrieved from https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html.

HHS Office of the Secretary,Office for Civil Rights, & Ocr. (2019, October 31). HIPAA Complaint Process. Retrieved from https://www.hhs.gov/hipaa/filing-a-c complaint/complaint-process/index.html.

Scalise, C. (2019, July 19). Hospitals Must Protect Patients and Their Information. Retrieved from https://thedoctorweighsin.com/hospitals-protect-patients-information/.

U.S. Department of Health and Human Services Office for Civil Rights Complaint Portal Assistant. (n.d.). Retrieved from https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf.

What are the Penalties for HIPAA Violations? (2019, November 11). Retrieved from https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/.

What is Considered Protected Health Information Under HIPAA? (2019, March 7). Retrieved from https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.