David McDaniel

ICTN 6810 / Tijjani Mohammed

HIPAA Rules and Current Threats for EHR's

Sunday, October 21, 2018

Abstract

People have placed a premium on the privacy of their health information for generations. For generations, people have been documenting medical history and incidents. Initially, this documentation was for didactic purposes, dating back to 1600 B.C. in ancient Egypt. With the onset of the Information Age and the explosion of Internet accessibility, electronic health records (EHR) has become the standard method of record keeping. The Health Insurance Portability and Accountability Act, also known as HIPAA, was signed into law 1996. In the years since, multiple refinements have been made to the law. In this paper, the author begins with an overview of both privacy and security as it relates to HIPAA. As the current security environment has seen a spike in medical record trafficking in criminal networks, electronic health record (EHR) systems are becoming increasingly targeted by malicious actors. In part II of this paper, the author provides a survey of current threats targeting the confidentiality, integrity, and availability of electronic health record (EHR) systems and their contained electronic protected health information (ePHI).

Introduction

The human race has long recorded information about medical history, procedures, and incidents. Even in 1600 B.C., surgical procedures were recorded on papyrus for teaching purposes (Gillum, 2013). In Information about one's physical and mental health is material that is most often considered to be very private. Most often, individuals do not want any conditions, discussions with healthcare providers, and more shared with unapproved parties. This fact, in conjunction with the massive quantities of non-medical data compiled into a patient's health record make the security and privacy of the containing systems paramount. For example, often a patient provides their healthcare provider with information regarding family members (e.g., parent's names including maiden name), financial information including credit card information for payment on the balance of their care, and even a patient's social security number. The accumulation of all of this information in one record is attractive for malicious actors since they would only need to breach one system to gain the information instead of finding multiple sources for information regarding the same individual. Once this information is collected, an attacker can easily impersonate the victim in order to steal their identity, opening financial accounts, loans, and using the information to further gain access to the patient by means of a trust-generating relationship.

PART I: Security and Privacy of Healthcare Systems under HIPAA

On August 21, 1996, President Bill Clinton signed into law the Health Information Portability and Accountability Act of 1996 (HIPAA) by the United States Congress (McLaughlin, 2013). As Andriole (2014) explains, this legislation was enacted for two primary reasons:

> (1) to protect health insurance coverage for workers and their families when they change or lose their jobs (Title I); and (2) to require the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers (Title II).

As part of the HIPAA legislation, the Secretary of Health and Human Services (HHS) was required to develop and publish privacy and security standards (Gallagher, 2010). Accordingly, the Secretary developed the Privacy Rule (originally published on December 28, 2000, then modified and finalized on August 14, 2002) and the Security Rule (published on February 20, 2003) (Mir, 2011). It is important to understand the differences between the terms *privacy* and *security* as it is defined under the HIPAA legislation as well as how they work together to protect patient confidentiality.

Privacy

The term privacy is used to indicate control over the confidentiality of data. In relation to HIPAA, privacy means that limits are enforced on uses and disclosures of protected health information (PHI) without the expressed consent of the patient (Office for Civil Rights, 2015). Although some exceptions are present, such as when worker's compensation cases are involved (McLaughlin, 2013) or for certain government functions and national security concerns (Rothstein, 2016), HIPAA guarantees the patient a right to maintain the confidentiality of their PHI. One particular exception to HIPAA's Privacy Rule is for research and reporting purposes. While in a general sense it is still required to obtain patients' authorization before PHI disclosure, in the event that this request would be unfeasible and the research does not pose a

significant risk to the patient's privacy, the disclosure is allowed (Cohen & Mello, 2018). However, as Cohen & Mello (2018) explain, if identifying information has been removed (e.g., name, date-of-birth, residency information smaller than a state, etc.) from the data set, it can be shared freely for research and even commercial purposes.

Security

The term "security" in HIPAA focuses primarily on the safety of electronic PHI (ePHI) while being stored or transmitted by a covered entity. HIPAA dictates that security safeguards are put in place to ensure that ePHI data under the CE's custodianship is protected from intentional or unintentional unauthorized disclosure, destruction, or modification (Sheffield, 2017). These safeguards are broken into three categories: administrative, physical, and technical (Shay, 2017). A sample of these safeguards is illustrated in Table 1. Administrative safeguards protect PHI by creating a standard to "implement policies and procedures to prevent, contain, and correct security violations" (Office of the Federal Register National Archives and Records Administration, 2007, p. 737). Physical safeguards are primarily focused on the security of the physical premises and electronic systems (e.g., servers, workstations, etc.). Technical safeguards are described as electronic measures to secure data from unauthorized access during storage or transmission.

Category	Safeguard	Example mitigation strategy
Administrative	Access Management	Establish and implement policies to control access to computer systems and applications
Administrative	Contingency Planning	Develop and implement a disaster recovery and incident response plan
Physical	Workstation Security	Prevent unauthorized physical access to computing terminals with access to PHI
Physical	Device Controls	Prevent the unauthorized removal of PHI-containing devices from the premises
Technical	Data Transmission Security	Properly encrypt all being transmitted which contains PHI.
Technical	User Authentication	Properly authenticate users based on passwords and/or other authentication methods

Table 1. Sample safeguards for administrative, physical, and technical categories (Shay, 2017)

PART II: Current Threats to EHR and PHI

As with many other industries, the source, vectors, and motivation of threats to healthcare networks are vast. Clearly, not all threat vectors can be delineated in a single paper. However below, the author introduces and explains several of the threats that currently pose the most risk to healthcare facilities. As will be demonstrated, not all threats to ePHI are of a technical origin. Often, the human is the weakest link in the security of information (Mahlaola & van Dyk, 2016). As Gordon, Fairhall, and Landman (2017) explain, employees are the largest risk to an organization, often allowing other sources of attack to succeed.

Ransomware

Ransomware is an attack where data is encrypted (or a user otherwise locked out from accessing the data) with the offer to purchase the decryption key to gain access (Allen, 2017). There is often a dilemma after a ransomware attack whether or not the organization should pay

the ransom to restore access to their files, or if the organization should attempt to restore from unaffected backups. Although this dilemma is outside of the scope of this paper, it should be understood that simply paying the ransom does not guarantee the receipt of a decryption key. Ransomware was first used to attack a healthcare facility when Surgeons of Lake County was attacked in 2012 (Spence, Bhardwaj, Paul, & Coustasse, 2018). Given that ransomware attacks have been increasing more than 500% each year since 2013 (Jung & Won, 2018), the threat to healthcare facilities is likewise growing exponentially.

Healthcare facilities are especially impacted by ransomware attacks for two reasons: (1) negative impacts on reputation and future profits and (2) the potential patient safety impacts of not being able to access a patient's records. Reputational impacts are particularly severe for medical facilities where patients often decide to switch to a competitor facility, resulting in irreparable harm in lost profits. The potential disruption in patient care delivery can result in putting patients' safety at risk (ECRI Institute, 2017). Almost exclusively, hospitals and surgical centers maintain surgery schedules and details electronically. A disruption of this information could result in a cancellation of surgeries, or, worse, an incorrect surgical procedure or wrong-site surgery resulting in serious patient safety concerns and, as a result, additional financial and reputational injury to the facility (Guy, Ghafur, Kinross, Hankin, & Darzi, 2018).

Mitigation strategies for ransomware attacks are primarily composed of two methods: (1) backups of critical files and systems and (2) user education to preemptively spot suspicious activity and avoid falling victim to the attack. It should be noted that backup devices should not be accessible via direct connection to the system or via the network as variants of ransomware (e.g., Locky) look to encrypt data on local devices, mapped devices, and even directories shared from other systems accessible by the compromised device (Sternfeld, 2017).

Insider Threats

Often times, security officers and information security administrators focus their efforts on attacks from outside of the organization, such as the ransomware threat explained previously. However, one of the largest threats comes from inside of a healthcare network, being introduced either intentionally or unintentionally (accidental or negligent) by the users of the information systems.

Intentional threats are a result of misuse of organizational privileges for malicious purposes. These intentional threats can be for a multitude of reasons with numerous goals. For instance, if a medical provider decides to leave the organization and start her own practice and takes patient contact information with them, or if an employee discovers that a celebrity or high-profile individual is being seen by an organization and inappropriately accesses the patient's health records, these can be seen as intentional threats. Additionally, more malicious acts could be involved such as the acquiring and selling of medical records by disgruntled employees.

Unintentional threats, although involuntary by nature, pose a significant risk to the security of medical records and health information systems. As an example, clinicians that fail to log out or lock computer systems when leaving an exam room could provide an opening for an unauthorized party to quickly gain access to the system. Also, improper disposal of medical records could result in PHI being accessed by unauthorized parties. These records need not be in the form of an electronic system, but could also be printed hard copies. In a study from November 2014 to May 2016, one research team found 2,687 documents which contained PHI, including 1,042 with highly sensitive data, in the recycling materials picked up at 5 teaching hospitals in Toronto (Ramjist, Coburn, & Urbach, 2018).

Finally, as a gateway to the network, people can inadvertently allow other threats to successfully enter the network. Phishing attacks and threats propagated through malicious email attachments rely on employees to involuntarily perform an action that allows an attacker to gain access to the information systems (Gordon, Fairhall, & Landman, 2017).

In order to combat the risk posed by insider threats, an organization should invest in a comprehensive security training program. Many threats can be diverted by an employee having the knowledge to identify threats (either from external sources or from malicious co-workers). Twiggs (2017) suggests that HIPAA training should be made into a fun and engaging activity (such as providing awards for individuals reporting internal email phishing scams conducted by IT as an exercise). In addition, implementing an auditing strategy where user actions are audited can be useful to lessen the risk posed by insider threats. Stafford, Deitz, and Li (2018) explain that it is necessary for complacent users to understand the importance of following the organization's security policy at all times, "even if they are safe not doing so" (p. 411).

Lost or Stolen Devices

Clinicians often use mobile devices such as laptops, tablets, and smartphones to assist in delivering patient care. Under the HIPAA provisions, the information stored on these devices should be encrypted (or otherwise protected) in case of loss or theft. However, in today's bring your own device (BYOD) networks, often this requirement is overlooked, particularly for employee-supplied devices. If these devices are stolen or lost, the penalties can be steep. In one incident, Children's Medical Center of Dallas reported an unencrypted BlackBerry was lost

which contained PHI for approximately 3,800 individuals, three years later a laptop with PHI for another 2,462 individuals was stolen, resulting in a penalty of $3.2 million (Lost Devices, 2017).

On September 12, 2016, Calyptix Security posted a review of data supplied by the United States Department of Health and Human Services' breach reporting portal between 2009 and 2016. Their review showed that theft was the cause of 44% of HIPAA breaches (Top 3 causes of HIPPA violations, 2016). As Calyptix (2016) explains, simply encrypting the data in a HIPAA-compliant manner on the device renders the lost information benign and frees the covered entity from having to report the breach. In fact, encrypting data on devices whenever appropriate is the most effective way to combat the threat of lost and stolen devices. Additional mitigation strategies include physical device security systems (e.g., cable locks for laptops) to prevent theft or loss of the devices.

Conclusion

Healthcare organizations, as with any other organization, face a multitude of internal and external threats to the privacy and security of patient data and information systems. The importance of securing this data cannot be overstated. Failure to thoroughly plan for these threats and implement the appropriate mitigation strategies can result in patient safety issues, financial repercussions, and reputational damage on the part of the organization. It is the author's hope that the information provided here demonstrate the severity of these threats and offer useful insight to the reader on a sampling of methods to mitigate the occurrence and severity of future information system breaches.

References

Allen, J. (2017, Summer). Surviving Ransomware. *American Journal of Family Law, 31*(2), 65-68.

Andriole, K. P. (2014, December 1). Security of Electronic Medical Information and Patient Privacy: What You Need to Know. *Journal of the American College of Radiology, 11*(12), 1212-1216.

Cohen, I. G., & Mello, M. M. (2018, July 17). HIPAA and Protecting Health Information in the 21st Century. *Journal of the American Medical Association, 320*(3), 231-232.

Discover the top 3 causes of HIPAA violations and their simple solutions. (2016, September 12). Retrieved from Calyptix Security: https://www.calyptix.com/hipaa/discover-the-top-3-causes-of-hipaa-violations-and-their-simple-solutions/

ECRI Institute. (2017, November). Ransomware and Other Cybersecurity Threats Top ECRI Institute's Annual Health Technology Hazards List. *Journal of Health Care Compliance, 19*(6), 39-40.

Gallagher, L. A. (2010, April). Revisiting HIPAA. *Nursing Management (Springhouse), 41*(4), 34-39. doi:10.1097/01.NUMA.0000370876.71090.03

Gillum, R. F. (2013, October). From Papyrus to the Electronic Tablet: A Brief History of the Clinical Medical Record with Lessons for the Digital Age. *The American Journal of Medicine, 126*(10), 853-857.

Gordon, W. J., Fairhall, A., & Landman, A. (2017, August 24). Threats to Information Security - Public Health Implications. *The New England Journal of Medicine*, 707-709. doi:10.1056/NEJMp1707212

Guy, M., Ghafur, S., Kinross, J., Hankin, C., & Darzi, A. (2018, June 4). WannaCry-a year on. *British Medical Journal (Online), 361*.

Jung, S., & Won, Y. (2018, October). Ransomware detection method based on context-aware entropy analysis. *Soft Computing, 22*(20), 6731-6740.

Lost Devices Lead to OCR Finding More Noncompliance. (2017, March). *Healthcare Risk Management, 39*(3).

Mahlaola, T. B., & van Dyk, B. (2016, December). Reasons for Picture Archiving and Communication System (PACS) data security breaches: Intentional versus non-intentional breaches. *Health SA Gesondheid, 21*(1). doi:10.1016/j.hsag.2016.04.003

McLaughlin, R. A. (2013, Winter). HIPAA, the privacy rule and their implications under the Longshore and Harbor Workers' Compensation Act. *Loyola Maritime Law Journal, 12*, 24-56.

Mir, S. S. (2011, March-April). HIPAA privacy rule: maintaining the confidentiality of medical records, Part I: a detailed look at the evolution of HIPAA privacy and how it impacts those it touches. *Journal of Health Care Compliance, 13*(2), 5-14.

Office for Civil Rights. (2015, April 15). *The HIPAA Privacy Rule.* Retrieved from U.S. Department of Health & Human Services.

Office of the Federal Register National Archives and Records Administration. (2007, October 1). *HIPAA Security Rule § 164.308(a)(1).* Retrieved October 21, 2018, from https://www.gpo.gov/fdsys/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1.pdf

Ramjist, J. K., Coburn, N., & Urbach, D. R. (2018, May 20). Disposal of Paper Records Containing Personal Information in Hospitals. *Journal of the American Medical Association, 319*(11), 1162-1163.

Rothstein, M. A. (2016, Summer). The end of the HIPAA privacy rule? Currents in contemporary bioethics. *Journal of Law, Medicine & Ethics, 44*(2), 352-358. doi:10.1177/1073110516654128

Shay, D. F. (2017, March 1). The HIPAA Security Rule: Are you in compliance? *Family Practice Management, 24*(2), 5-9.

Sheffield, J. (2017, December). Pirates of the PHI: Identifying and Responding to a Ransomware Attack According to HIPAA Best Practices. *Benefits Law Journal, 30*(4).

Spence, N., Bhardwaj, N., Paul, D. P., & Coustasse, A. (2018, Summer). Ransomware in Healthcare Facilities: A Harbinger of the Future? *Perspectives in Health Information Management*, 1-22.

Stafford, T., Deitz, G., & Li, Y. (2018, April). The role of internal audit and user training in information security policy. *Managerial Auditing Journal, 33*(4), 410-424. doi:10.1108/MAJ-07-2017-1596

Sternfeld, U. (2017, January 5). *How to defend against ransomware targeting shared network drives and cloud backups*. Retrieved from Cybereason.

Twiggs, M. (2017, May). Preventing insider HIPAA violations. *Briefings on HIPAA, 17*(5), 9-11.