Privacy and Security Issues Faced with the Implementation of Electronic Health Records

Blaine Reichart

University of Saint Mary

Synopsis

In 2004, George W. Bush ordered that the American health-care industry must implement electronic medical records (EMR) by the year 2014 (Hoffmann, 2009). Those that did not comply would face hefty fines. With this proclamation came the issue of how to securely protect this information which would now be easier accessible compared to the previous paper records. In the wrong hands, this information could be devastating and can inflict financial harm on patients, providers, and insurers. In addition, some hackers corrupt records with erroneous information that can lead to incorrect diagnosis and treatment (McNabb & Rhodes, 2014). Not only are organizations being fined if they have not implemented EMRs but those who have implemented unsuccessful EMRs that do not comply with the Health Information Technology for Economic and Clinical Health Act (HITECH) also face fines. This act gives the U.S. Department of Health and Human Services Office of Civil Rights (OCR) the right to increase the monetary penalties towards organizations that violate the Health Insurance Portability and Accountability Act (HIPPA) (Zamosky, 2014). Simply put, the healthcare industry is feeling the pressure and the wrath of EMRs. Frequently we hear about how a healthcare organization has failed to safeguard the privacy and security of patient data. Securing this sensitive information and preventing data breaches has become more complex (Zamosky, 2014). Medical identity theft has been defined as the fraudulent use of healthcare information and is described as the privacy crime that can kill you (McNabb & Rhodes, 2014). There are primarily two ways medical identity theft happens: consensual and nonconsensual. Consensual theft occurs when an individual knowingly shares their identifying information with others whereas nonconsensual happens when someone unknown to the victim gains access to their medical records. With computer networks, EMR can easily be accessed and copied unlike paper records which are cumbersome. With the nationwide implementation of EMRS and multiple reports of data breaches, health care organizations must beef up their security measures in order to protect their patients and employees from medical theft.

Time Context of Problem

The issue of properly securing EMRs should be addressed immediately by healthcare organizations that lack the security needed to protect this sensitive information. Every organization must individually determine how much IT security is appropriate and the amount of risk they are willing to take (McMillian, 2015). After establishing the amount of IT security, the implementation phase should quickly begin and take a matter of weeks. Support from the different branches of the organization will ensure that this process is completed smoothly.

Case Viewpoint

While healthcare organizations are the obvious owners of this problem, other less apparent owners exist. All healthcare providers, payers or customers, and policy makers are owners of medical identity theft. Anyone who is involved in the exchange of health care information should recognize the damaging effects the misuse of this information could have and therefore learn the risks and recommendations for protecting it from medical identity theft. All of these owners must work together in order to ensure any medical identification theft is promptly noticed and dealt with before the breach of information becomes damaging to the individual. According to McNabb & Rhodes (2014) “ 34 percent of victims reported discovering the crime one year after the incident while 17 percent reported discovering it two or more years” (p 29). This statistical report is staggering considering the amount of harm that could potentially come to patients impacted by medical identity. This harm includes, but is not limited to, loss of privacy and confidentiality, denial of benefits, possible legal action or false arrest, loss of credit, lost time and money, and impaired health resulting from improper treatment (McNabb & Rhodes, 2014).

Problem

The main deter that prevents health care organizations from implementing a proper IT security system for the protection of health records is related to the financial aspect as well as lack of policy and laws governing this area. Data loss prevention (DLP) tools allow organizations to accurately track and control the location of medical information. As a result, inappropriate actions or breaches are avoided. Unfortunately, the financial impact this has on an organization can run from $150,000 to more than $1 million depending on the size. For a small, community hospital this is a large amount of money that may not be readily available and therefore an unrealistic solution. One of the main difficulties is the lack of protocols and standards. There are no standard protocols across the board and each state policy regarding the collection, exchange, and retrieval of electronic health information varies. In addition, a more basic privacy-related challenge stems from the delivery of healthcare and how it is determined which providers can access patient data. A small number of hospitals have created a system that grants and revokes patient data access on a daily and hourly basis in order to protect against medical identity theft (Hoffmann, 2009). It is an imperfect system that must be balanced in order to protect sensitive information while at the same time continuing to give patients the very best care.

Objectives

In order to combat the problem of medical identity theft, certain goals must be accomplished. These include an industry wide approach that includes the implementation of policies and procedures for the prevention, detection, and mitigation of medical identity theft as well as the goal of engaging consumers in preventing theft. In order to successfully tackle this privacy crime, there needs to be collaboration among all healthcare industry stakeholders (McNabb & Rhodes, 2014). Building awareness and implementing an identity theft response plan to address potential indications of medical identity theft is the primary recommendation. An increase in protection and security of patient EMRs nationwide is the final result that needs to be accomplished. I believe healthcare organizations owe this security to their customers

Area of Consideration

I. STATISTICS OF MEDICAL IDENTITY THEFT

a. In 2013, 1.84 million people found themselves as victims of medical identity theft which was a 21 percent increase over the previous year (McNabb & Rhodes, 2014).

b. 34 percent of medical identity theft victims reported discovering the crime one year after the incident while 17 percent reported discovering it two or more years (McNabb & Rhodes, 2014).

c. 8 percent of patients state that they felt that a healthcare organization had improperly disclosed their personal medical information. As a result, 13% of all patients admit to avoiding medical tests in an effort to engage in privacy-protecting behaviors.

d. Most organizations say that they only spend 6 to 12 percent of their IT budget on security measures (McMillan, 2015).

II. REASONS OF MEDICAL IDENTITY THEFT

a. EMRs can easily be accessed and copied compared to the past paper record.

b. Lack of appropriately trained staff regarding medical identity theft. The misuse of data by employees is a main cause of breaches. 57 percent of employees stated that they were unaware of their organization's current security policies and procedures (Zamosky, 2014).

c. Data loss prevention (DLP) and other security systems can cost an organization between $150,000 to more than $1 million.

d. Multiple state laws have been developed to tackle the issue of data privacy but unfortunately are inconsistent due to the fact that data networks cross state lines. No comprehensive federal privacy laws have yet to be enforced.

III. EFFECTS OF MEDICAL IDENTITY THEFT

a. Misuse of sensitive information can be devastating to an individual's reputation and can affect all aspects of their life.

b. When an EMR security incident occurs, a healthcare organization will incur direct costs associated with the discovery, response, and investigation (McMillan, 2015). These costs can run from a couple hundred to millions of dollars. A breach requires organizations to notify patients, the government and often the media.

Alternate Courses of Action

Healthcare organizations can chose to fully protect their patient's sensitive medical information to the best of their ability or implement the least amount of IT security required by the organization. Since federal laws related to EMR security have yet to be put in place, healthcare organizations are given the full responsibility of assessing their system and concluding what level of security to implement. Two very different cost profiles related to EMR security are available: a proactive approach and an approach reactively in response to a security breach or compromise. A proactive approach initially has a larger upfront cost from the organization and is implemented as a preventative measure (McMillan, 2015). If an EMR security breach occurs due to lack of implemented security, the reactive response approach will be much more costly to an organization.

Conclusion

As fines continue to increase for healthcare organizations that violate HIPPA rules, the complexity of preventing data breaches also continues to escalate. Pressure is mounting for all healthcare organizations to install an IT system that safety monitors health information in an effort to decrease and avoid medical identity theft. This theft can be devastating to an individual and organizations should take measures to protect their patients from this disaster. Medical identity theft not only inflicts financial and emotional harm on individuals but it also corrupts records with erroneous information that can lead to incorrect diagnosis and treatment (McNabb & Rhodes,2014). Policies and procedures must be put into place within the organization in order for employees to recognize potential data breaches. In addition, any patient complaint regarding an EMR breach should be processed quickly so that the theft team can investigate thoroughly through reviewing the patient’s medical records and other documentation (McNabb & Rhodes, 2014). I believe that if a proactive approach was implemented across all healthcare organizations, the medical identity theft rate would decrease as well as the hardship felt by those who fall victim. Every organization needs to investigate their EMR security system and assess each feature thoroughly in order to ensure the very best results for their customers (Mendoza, 2003).

Recommendations

For ethical and practical reasons, as well as to avoid potential legal liability, many organizations have instituted policies designed to protect patient information. The healthcare industry must collaborate in order to tackle the crime of medical identity theft. In order to securely protect EMRs within the clinical setting, I propose that healthcare organizations promptly (within a 6 month time frame) implement the following recommendations if not currently being used.

- Patients should be advised by healthcare organizations as to who has access to their EMRs. Levels of access to this sensitive information should be specifically identified for every employee. Training regarding IT security should be provided to every employee and a written confidentiality policy must be written and enforced. Admitting and registration staff should be trained on how to monitor for suspicious patterns or practices while employees in the coding and business office should be able to recognize medical record inconsistencies that may point to a breach in EMRs. Organizations need to frequently remind employees of their obligation of confidentiality. All extremely sensitive healthcare information should be flagged with a warning notice emphasizing potential liability for unauthorized disclosure.
- Patient should be given the opportunity to discuss with their physician what personal information they do not want distributed via EMR systems. Patients should be made aware that they will not have total control over their records. For example, federal law and government agencies require healthcare organizations to report specific incidents and positive tests including HIV, meningitis, stabbings and gunshot wounds.

- Healthcare organization should conduct a security risk analysis. This assessment is intended to accurately identify potential risks and vulnerabilities to the confidentiality, integrity and availability of EMRs within the organization (Workman, 2016).
- Meaningful notice should be given before patient-specific information is released to data clearinghouses.
- Strict security procedures should be in place in order to prevent unauthorized access to EMRs. EMR auditing procedures should also establish in the event of unauthorized disclosure of personal information. Terminated employees should immediately be removed from having access to patient data from EMRs.
- Whenever patient data is transmitted electronically from one location to another, data should be encrypted.
- Unannounced security audits should be performed. These audits should be an evaluation of whether written policies and procedures are being followed correctly by staff. Healthcare organizations should consider hiring a hacker to attempt to break into the computer system and access EMRs. If successful, the hacker can advise the organization on how they accomplished entry and those security issues can be addressed promptly.
- Data loss prevention (DLP) systems should be installed in order to help the organization avoid inappropriate actions or breaches by identifying and managing all sensitive information, both in databases and unstructured files, as well as monitoring the flow of information and enabling end-point protection to guard against data loss.
- Cyber insurance should be considered to cover gaps and financial costs if a security incident does occur.

References

Hoffmann, L. (2009). Implementing electronic medical records. *Communications of the ACM*, 52 (11), 18-20. doi:10.1145/1592761.1592770

McMillan, M. (2015). The cost of IT security. *Hfm (Healthcare Financial Management),* 69(4), 44-47. Retrieved from https://stmary.idm.oclc.org/login?url=http://search.ebscohost.com /login.aspx?direct=true&db=buh&AN=101847404&site=ehost-live

McNabb, J., & Rhodes, H.B. (2014). Combating the privacy crime that can kill. *Journal of AHIMA / American Health Information Management Association,* 85(4), 26-29. Retrieved from http://stmary.idm.oclc.org/login?url=http://search.ebscohost.com /login.aspx?direct=true&db=cmedm&AN=24834550&site=ehost-live

Mendoza, E. (2003). Security considerations when choosing an EMR system. *Health Management Technology,* 24(10), 48. Retrieved from https://stmary.idm.oclc.org/login ?url=http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=10957540&site= ehost-live

Zamosky, L. (2014). Avoid the breach: Put data security measures in place. *Physician Executive,* 40(4), 82-84. Retrieved from https://stmary.idm.oclc.org/login?url=http://search. ebscohost.com /login.aspx?direct=true&db=buh&AN=97122565&site=ehost-live