Security of Health Care Information System

[Student's Name]

[Institution Affiliation]

Abstract

Recent empirical research indicates that many health care organizations have moved from paper-based health care information systems to electronic ones. This is after paper-based health information system has proven inadequate to handle the increasing needs of health care information and the many limitations associated with it, such as errors, and lack of proper access among others. Electronic health care information system has various benefits, but on the other hand, it is highly vulnerable to many security threats. These security threats led to the development of various security standards to enhance the protection of electronic health information. In relation to this, this paper aims to present the various security threats to electronic health information, which make it a necessity for all healthcare providers to develop and implement a security program to enhance protection of their health information. The paper will briefly explain some of the administrative, physical, and technical standards set by Health Insurance Portability and Accountability Act (HIPAA), to enhance the protection of healthcare information system. The paper will also discuss the various threats posed to emerging technologies, such as wireless and remote technology. In conclusion, the paper will explain the various implications of the current security issues with health care information and recommend the future direction to be taken.

Introduction

Research shows that almost all health care organizations worldwide have stopped using paper-based medical records and adopted the use of Electronic Medical Records (EMRs). This is after paper-based recording of medical information proved inadequate due to the increasing information medical information needs. It is also argued that paper-based recording of medical information has various shortcomings. These include difficulty in accessing the records from multiple locations, loss of some valuable health records, errors in recording the information and tiring. With EMRs, medical information can easily be accessed from various locations and losses have greatly been minimized. However, empirical research shows that even EMRs are vulnerable to various threats such as computer viruses, fire in the computer room, and loss of medical information through employee theft, just to mention but a few. Therefore, organizations must make it a priority to establish a security program of ensuring that medical records are protected from such threats.

Background Information

According to Meingast, Roosta, and Sastry (2006), security issues with health care information have existed for several decades. Even before health care organization adopted the electronic technologies for gathering, recording, transmitting, and storing medical information, the paper-based healthcare information was also vulnerable to various security threats. The adoption of electronic health care information by many health care organizations has been on the rise in the last decade. Currently, it is argued that more than 90% health care organizations use electronic technologies for their health care information systems.

According to Appari and Johnson (2010), over the past two decades, many studies have been conducted on security issues in relation to electronic health care information system. It is

debated that many of the researches have focused on analysis of security risks associated with electronic health care information. Some few researchers have focused on some solutions for the present security threats to electronic health information. However, it is clear that few if any researches have focused on the development and implementation of effective security programs, which can be used in enhancing protection of electronic health care information system. In relation to this observation, this paper addresses the various security issues that make the development and implementation of a security program a necessity in the present health care organizations.

Importance of Health Care Information Security Program

Having a security program in any health care organization is important, as it ensures that any threats to medical information are realized early enough and hence the negative impacts avoided. According to Wager, Wickham, and Glaser (2009), many health care organizations relax after adopting EMR for their recording, storage, retrieval, and transmission of medical information. However, they fail to realize that even EMRs are susceptible to the above already mentioned threats. As these authors explain, these are not the only threats to electronic medical information. Some threats might be intentional or unintentional damage or misuse of hardware, software or even the stored data. If such threats are not recognized before they occur, they can totally paralyze the information system of a health care organization. Taking for instance, if computers in a health care organization are destroyed, the organization is greatly affected, and it might even be forced to close down for some days. If personal health information is lost through burglary, the organizations may lose its clients. All these factors explain the importance of having a program that ensures security for electronic medical information.

According to Wager, Wickham, and Glaser (2009), the main function of a security program is to identify these threats and hence come up with processes or mechanisms through which these threats can be avoided or mitigated. Some of these processes or means of avoiding threats include installation of computers with anti viruses to prevent them from being attacked by viruses, having security codes to protect medical information from being accessed by anyone and hence securing the information from possible theft. Ensuring medical information security is important not only to the organization but also to the patients. Securing medical information ensures that the patients are assured of privacy, which is important to them. The security program therefore, ensures that private patients' medical information is not accessed by anyone or misused for any personal gains. As Wager, Wickham, and Glaser (2009) explain, it is important that the program is not only designed to protect patients' medical information, but also protect all the IT assets of an organization's information system from all potential threats, both human and natural.

According to Anderson (2004), developing and implementing a security program in an organization is challenging, especially in balancing its needs for security and the costs incurred. The initial costs for developing and implementing an effective security program are high. These expenses shun away some organizations from developing a security program. However, once in place, the expenses saved by an organization cannot be compared with the development costs incurred. If for instance the network of an organization is tampered even for some few hours, the losses incurred are huge. If personal health information belonging to the patients is accessed by an unauthorized user and misused, the organization loses these patients because of lack of privacy for their medical information they have entrusted the organization with. The dilemma many organizations undergo through when choosing whether to implement a security program

for their medical information or not is the same as that undergone by a person when choosing whether to take a long-term care insurance or not. People fail to see the potential expenses, which will be incurred in ensuring good health in the future.

According to American Nurses Association (2008), the main importance of good management of health information and records is to facilitate quality care for the patients. Therefore, one feature of this challenge is to maintain a proper balance between the security of health care information system and the availability of the health care data and information. A security program for health information ensures there is no unrestricted access to patients' health information to guarantee the privacy of the medical information is not compromised. On the other hand, organizations should be very careful while designing their security program for their medical information so that it is not so strict. If the security program is very strict, it may hinder the proper access to health information, essential in ensuring quality care for the patients. This shows that the security program should strike a balance between access and security in such a way that there is enough privacy for the patients' medical information and, on the other hand, there is proper access to these records to secure proper care for the patients.

Potential threats to Health Care Information

According to Gina (2005), health care information is vulnerable to many threats. However, it is possible to categorize these threats into three main categories. The first category is comprised of the threats created intentionally or unintentionally by human beings. Intentional threats mean that a person tempers with the information system knowingly for his or her personal gains without minding the damages the information breach will have on the organization as a whole. On the other hand, a person may mess health care information system

without his or her knowledge, such as the use of software, which contaminates the computers with a virus leading to data loss.

These threats can originate within the organization that is caused by the employees or externally, by individuals outside the organization. Intentional threats include deliberate alteration of health data, its destruction or stealing. This is possible through an employee within an organization or a computer hacker outside the organization. In the United States, cases of loss of health records through stealing and alteration of health information through computer hackers are rampant. A good example is a recent case in Florida, where a daughter to a hospital employee had accessed the health information of some patients who had recently visited the institution. She went ahead, used their phone contacts, and called notifying them they had tested HIV positive. It is argued that most of the contacted patients became depressed before it was disclosed to them that it was the wrong information. The hospital lost most of the clients.

According to Huffman (1994), viruses are among the most common intentional computer interferences in the society today. The damages caused by viruses are great. Viruses may lead to health data loss without any possible recovery. It can also cause a total crash down of the whole health care information system. People create attractive adverts and messages with highly damaging viruses and post them on the net to put many computer users at the risk of opening them, and hence infected. Many people doing this are the anti-virus producers in an attempt to obtain more customers for their products. Research points out that most of the unintentional threats to health care information system are caused through human errors or improper use because of lack of proper training. Users may share passwords or access information from a non-secure site creating possible security breaches to the information system.

As Huffman (1994) explains, internal security breaches are common, when compared to external breaches. Research points out that, cases of health care organizations' employees having illegally used patient's health information have become common. Some corrupt clinical employees are given bribes to access patient information for legal cases. Internal security breaches can also occur through installation or use of unauthorized software, which introduces viruses into the computing system. Hackers accessing the health information without any authorization mainly cause external security breaches. E-mail harassment and porn surfing also constitute to some of the external security breaches. Not only computer software, which is vulnerable to security threats, but also computer hardware is susceptible to robbery, leading to the loss of computers and, hence, loss and possible exposure of confidential health information stored in them.

The second category of security threats is composed of natural or environmental catastrophes such as floods, fire, or power shortages. In relation to this, the security program should come up with storage devices that can be used to store back up health data if such disasters occur. The other category is made up of the threats caused by technology failure, such as a drive crushes down in absence of back up. Research indicates that Electronic Health Records are vulnerable to all these threats. Whether intentional or unintentional, these threats cause serious damages to health care organizations whenever they occur. In relation to this, all health care organizations should establish and implement effective administrative, physical, and technical security safeguards to ensure that confidential and important patients' health information is properly secured. As a result, the Department of Health and Human Services established security standards, under the conditions of Health Insurance Portability and

Accountability Act (HIPAA), which provides the framework for developing an effective security program for a health care organization.

The HIPAA Security Rule

According to Quinsey (2004), the HIPAA Security Rule was published in the Federal Register on 20 February, 2003. Before 2003, the same Security Rule had been published in 1998, but it faced much resistance, as health care organizations claimed that it was too prescriptive and, hence, rigid. Therefore, the rule published in 2003 is argued to be flexible as it only guides health care organizations on what should be done and not how to do it. As Quinsey (2004) explains, the rule outlines the various administrative, technical, and physical security measures that should be taken by all the covered entities to ensure that electronic medical information and records are properly protected. According to Anderson (2004), a Covered Entity (CE) can be described as any health care provider or healthcare plan, which transmits secured health information in electronic form. HIPAA Security Rule standards can be divided into four main categories:

a) The Administrative Safeguards

The administrative safeguards contain various security standards. The first standard is on security management functions. Every covered entity should ensure that effective policies and measures are implemented to detect, prevent, mitigate, or correct any security breaches. In order to do this, a CE should conduct a thorough analysis of the potential risks to confidentiality, availability, and integrity of electronic health information. After identifying and analyzing all potential risks, a CE should implement various measures aimed at managing the identified risks. It is also an obligation for the CE to implement various policy sanctions to punish any employee not adhering to the set rules and regulation regarding security of health

information. It is also mandatory that the CE must regularly review the health information systems through audit and assessment reports to ensure that the administrative security standards are not compromised at any time.

The other administrative security standard requires a CE to identify a person, who will be responsible for developing all the security policies and regulations. The other standard under this category requires a health care organization to ensure that its entire workforce has proper access to electronic health information. On the other hand, it also requires the health care provider to guarantee that unauthorized people do not access the electronic health information. The other standard originates from the access to health information. The CE must secure that the workforce has proper access to health information and at the same time prevent unauthorized people from accessing it. The policies and procedures are implemented for ensuring that the access to health information is managed effectively.

As indicated earlier, some threats to heath information are created through human errors and improper use of electronic health records because of lack of enough training. In relation to this, the other administrative security standard requires a security plan to have policies that ensure the workforce to undergo adequate training on the proper use of the electronic health information system. The training programs should focus on issues such as password management, log-in procedures, and ways of avoiding insecure internet sites and installation or use of unauthorized software. A health care provider is also required to develop and implement policies, which ensure that all security incidents are reported and documented. This will help in tracking the pattern of security breaches in a particular health care organization and, hence, develop the best measures of avoiding their repetition in the future. Every covered entity should also have a contingency plan that ensures: a plan for data back up, a plan for recovering any

lost or destroyed data, a plan for operations during emergency time e.g. power shortages, have procedures for testing and revision of health information and finally, a plan for analyzing the various applications of the available health information. The evaluation standard is important, as it ensures that technical and non-technical periodical evaluations are carried out to detect any changes that might affect the security of the electronic health information and records. The last but not the least standard under administrative category requires a CE to develop arrangements and other business associate contracts. Such arrangements would clearly establish conditions under which electronic health information and records can be released or exchanged.

b) The Physical Safeguards

According to Amatayakul (2005), the main standard under this category requires a health care provider to ensure there is enough access control to all security facilities within a health care organization. This is possible through implementation of policies that limit physical access to an organization's electronic health information systems and the facilities in which they are stored. It is important that the organization sets limits on whom and when the personnel are allowed to access the electronic health information system. A health care provider should validate access of various employees to electronic health information or the facilities in which they are stored, based on their roles. For instance, it is important that personnel in charge of information management and recovery have proper access to the information system facilities almost all the time. Every CE should keep maintenance records, which document all the modifications or repairs to physical machinery of the information system facilities to enhance the physical security.

The other physical security standard entails workstation use. A health care provider is required to establish policies that clearly indicate the functions that should be performed in a

particular workstation, used in accessing electronic health information system. The manner in which they are supposed to be performed should be clearly specified. The physical characteristics of the surroundings of the workstation should also be specified to enhance the physical security. The other standard makes it mandatory for a CE to ensue that the workstations are under tight physical security. The access to these workstations should be restricted only to the authorized users. As Amatayakul (2005) explain, the other standard under this category involves good management of media and device controls. A health care provider should ensure there is tight physical security when hardware and electronic media containing electronic health information is being moved into and out of a facility or being transferred between facilities.

It is also mandatory that a CE ensures that the hardware or the electronic device used for storing health information is properly disposed after it is permanently damaged or worn-out. In case the electronic media is to be reused, a health care provider should ensure there are processes used to safely remove the electronic health data stored in them. It is important that the health care provider is accountable for all the movements of hardware and electronic media containing health information and be aware of the person responsible for the movements to easily follow up in case the hardware or electronic media is interfered with in the process of movement. Before the movement of hardware and electronic media, it is required that the CE produces an exact copy of the electronic health care data being moved for back up purposes on condition that anything goes wrong and the data is ether lost or damaged.

c) The Technical Safeguards

According to American Nurses Association (2008), a CE must ensure there are technical policies and procedures that ensure proper access to electronic health information system. In

relation to this standard, a CE is required to use unique numbers or names that can be used in identifying and tracking each user. There should be developed the procedures, which could be used in obtaining the electronic health information in case of an emergency. A health care provider is also encouraged to have automatic log-offs, which ensures that the system goes off on its own after a specified period of inactivity. It is also mandatory for a health care provider to develop and implement policies that govern the encryption and decryption of electronic health data whenever needed.

A health care organization is also required to conduct audit controls that examine and record all the activities taking place with information system containing electronic health information. The other standard under this category requires a CE to guarantee integrity of electronic health information by implementing policies, which ensure proper protection of the electronic health data from potential loss destruction or alteration. There should be policies and procedures that scrutinize the actual identity of a person or user seeking to access electronic health information. The other technical standard entails transmission security. Every CE is supposed to implement policies and procedures which ensure that electronic health data being transmitted over a network is properly protected from any alteration without detection. To make this possible, the health care provider is supposed to encrypt electronic heath data where it is considered appropriate.

d) Policies, Procedures and Documentation Standards

Under these standards, a CE is supposed to develop and implement policies and procedures that comply with all the set standards and requirements. The documentation standard requires a health care provider to ensure that all the policies, as well as procedures, implemented to comply with the security rule standards are maintained in the written form. The CE is required

to maintain and retain the documentation for a period of six years before discarding it. The CE is also required to make the documentation available by providing it to the people in charge of developing and implementing the security policies and procedures. It is also mandatory that the CE must review the documentation regularly and update it whenever required.

Wireless Environment Security

Empirical research argues that wireless technology is greatly influencing the operations of health care information system. According to Waller, Adele, and Oscar (1998), wireless technology has made health care providers flexible and enhanced their capability. Because of their various benefits, many health care providers have adopted it at a high rate. This has however resulted in many concerns, especially in relation to the security threats they present to health care information system. As these authors explain, the main problem with wireless security is that it is difficult to limit the transmission media only to the areas under a CE's control. In relation to this, wireless technology is vulnerable to various security threats.

One common security threat is unauthorized access to an organization's computer networks by malicious entities using wireless connections, as they can easily sidestep firewall protections. It is also argued that sensitive health information, which is not encrypted, can be easily intercepted and disclosed during the transmission process between wireless devices. Wireless connections are highly vulnerable to DoS (denial-of-service) attacks. With wireless devices, in case the health information is not properly encrypted, it can easily be corrupted by malicious entities. Research shows that portable wireless devices such as laptops can easily be stolen and sensitive health information may be exposed. The wireless devices are not only susceptible to external attacks but also internal attacks through ad hoc transmission. Unauthorized people might easily gain access to a wireless connection through war driving.

In relation to these threats, Wireless Equivalent Privacy (WEP) was developed to ensure that wireless technology was protected. However, research indicates that WEP has been associated with various limitations. Some of these shortcomings, including security attributes in many WEP retailer products, are not enabled; the cryptographic keys are shared, short and cannot be updated automatically. As a result, WiFi Alliance created WPA, which replaced WEP. Despite the installed security safeguards against security threats, it is important that all health care organizations using wireless technology must ensure that all potential risks are properly analyzed and managed. As Murer et al. (2000) explain, it is important that a health care provider develops and implements policies and sanctions to guarantee that any employee who misuses wireless technology or uses it illegally is punished accordingly.

Remote Access Security

According to Waller, Adele, and Oscar (1998), globalization and modernization has affected health care organization just like any other organization in the modern society. Various modern health care organizations are allowing their employees to work from home or any other place outside the organization. However, research points out that the remote technology has added security issues to the health care information system. There have been many cases in relation to remote use of devices, such as laptops used to store important electronic health care information. The potential threats to remote technology include loss of the portable remote devices through theft, loss of password or log-in information, resulting to potential illegal admission to electronic health data, while working offsite among many others. Some of the solutions to the mentioned threats include installation of personal firewall protection on all laptops that are used to access electronic health information, both inside and outside the health

care organization. It is also important that all the health care employees aree properly trained on how to use remote technology before they are authorized to have access to it.

Implications of Health Care Information System Security Issues

According to Mishra et al. (2011), technological advancement has greatly affected health care information system. Various advantages are presented by electronic health information technologies that have promoted their adoption by many health care organizations. However, it is clear that the electronic advancement poses serious challenges in terms of patient privacy and security of important electronic health care information. As technology advances, the security issues with health care information become more complex. This observation implies many things, especially to all health care providers.

Despite that, these new technologies provide many benefits to health care providers, various security issues should first be explored to promote the ethical principles that govern health care information. Some of the issues that must be carefully assessed include: access control, security of electronic data transmission, data analysis, the governing policies and procedures. It is clear that there are regulations and policies already in place that ensure the protection of electronic health care information. However, there is a great need to reevaluate these regulations and polices to ensure maximum security of health care information. Developing and implementing a security program for health care information system may be expensive, but it is important that all health care providers make it a priority. It has already been shown that electronic health information is susceptible to many security threats, which can have devastating effects on patients and the health care organization.

Conclusion and Future Recommendations

From the above literature review on security issues with health care information system, it is clear that may organizations have adopted electronic recording, transmission, and storage of their health information and records. Electronic technologies enhance the access and minimize manual errors with heath care information. The emerging technologies, such as wireless and remote networks have added several benefits to health care providers. However, they have presented more security issues in relation to patient privacy and security of electronic health care information. It is evident that the electronic health information system is highly susceptible to multiple security threats. These threats include theft, unauthorized access, damages through human and technical errors, destructions through natural disasters, such as fire and floods among others. In relation to security of health care information, HIPAA formulated various standards that govern healthcare providers on various administrative, physical and technical policies and procedures, which ensure the integrity and security of health care information is safeguarded.

Whether intentional or unintentional, these threats pose serious negative effects on any health care organization. It is of great significance that health care providers develop and implement an effective security program that protects electronic medical information from the already mentioned threats. HIPAA has set the groundwork of security standards, but some areas can be improved in the future. Health care providers should set more clear rules that define the attributes of role-based access to electronic health information. As the information needs of health care organization are expected to continue increasing, there is a need for new policies and standards to be developed to enhance the security of health care information system. Clearer guidelines need to be set, which will regulate the patient’s privacy while at home and the extent of control he or she has over the medical information.

References

Amatayakul, M. (2005). Access controls: striking the right balance. *Journal of AHIMA* 76(1), 56–57.

American Nurses Association. (2008). *Nursing informatics: scope and standards of practice.* Silver Spring, MD: Author. (ISBN 978-1-55810-256-9).

Anderson, E. M. (2004*). Online clinical documentation in the electronic legal medical record.* 2004 IFHRO Congress and AHIMA Convention Proceedings.

Appari, A., & Johnson, E. M. (2010). Information security and privacy in healthcare: current state of research. *Int. J. Internet and Enterprise Management,* 6(4), 279-315.

Gina R. (2005). The prompt, the alert, and the legal record: documenting clinical decision support systems. *Journal of AHIMA* 76(2), 24–28.

Huffman, E. K. (1994). *Health information management,* 10th ed. Berwyn, IL: Physicians' Record Co.

Meingast, M., Roosta, T., & Sastry, S. (2006). *Security and privacy issues with health care information technology.* Proceedings of the 28th IEEE EMBS Annual International Conference New York City, USA**.**

Mishra, S., Leone, G., Caputo, D., Calabrisi, R., & Morris, R. (2011). Security awareness for health care information systems: a HIPAA compliance perspective**.** *Issues in Information Systems,* 12(1), 224-236.

Murer, C., Murer, M., Brick, L. (2000). *The complete legal guide to healthcare records management*. Washington, DC: Healthcare Financial Management Association.

Quinsey, C. A. (2004). A HIPAA security overview. *Journal of AHIMA,* 75(4), 56A–C.

Wager, K., Wickham, F., & Glaser, J. (2009). *Healthcare information systems: a practical approach for healthcare management.* San Francisco, CA: John Wiley & Sons. (ISBN 978-0-470-38780-1.

Waller, A., & Oscar, A. (1998). Ownership of health information in the information age. *Journal of AHIMA*, 69(3), 28–38.