SECURITY ISSUES, CHALLENGES, AND SUCCESS FACTORS OF HOSPITAL INFORMATION SYSTEM

By

AMAL KRISHNA SARKAR * R. A. KHAN ** C. M. PANDEY ***

* Research Scholar, Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, India.
** Professor & Head, Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, India.
*** Professor & Head, Department of Biostatistics and Health Informatics, Sanjay Gandhi Postgraduate Institute of Medical Sciences, Lucknow, India.

Date Received: 13/09/2017 Date Revised: 26/09/2017 Date Accepted: 18/10/2017

ABSTRACT

The utility of Hospital Information System (HIS) is vast, although one cannot ignore its challenges which prevent the electronic healthcare system from being used properly. Challenges in privacy and security of HIS needs to be studied and understood properly by any healthcare organization and should be resolved to get optimum benefit. One of the main objectives of this paper is to review, explore and analyze the current state of hospital information system's privacy and security of patient's electronic health records. It also focuses on security at the level policy of healthcare organization so that electronic patient record can be protected and secured. In healthcare organization security risks and financial consequences are increasing day-by-day. The vulnerable and breached electronic patient data revealed the fact that, the privacy and security of electronic patient records in health information exchanges is an imperative of any healthcare organization. For any patient care organization persons who are involved in the IT and administrative management should seriously think the issues of privacy and security of patient health record and also proper health information exchange in a secured manner.

Keywords: Hospital Information System, Cryptography, Electronic Patient Record, Electronic Medical Record, Information Exchange.

INTRODUCTION

Until recently, IT products available for healthcare providers were mostly designed for large organizations and were costly [1]. Healthcare security is different from security of other industry. It has legal issues, regulated (HIPAA- Health Insurance Portability and Accountability Act of 1996) and do not have bilateral conditions. People in healthcare set up is becoming more and more conscious about the smooth functioning of HIS and its security, privacy issues, and challenges. Because of its several challenges, the vast usage of e-health system is still at an early stage and is growing day-by-day. Managers in healthcare domains need to identify the threats to healthcare assets. Providing an up-to-date category of threats can help to highlight the role of human in different threats to HIS [2]. Based upon the evidence in the practitioner literature, the next two decades will mark a large surge in the number of medical practices implementing Electronic Medical Records (EMR) systems. This research treats EMR systems as medically oriented Enterprise Resource Planning (ERP) systems and draws upon that literature to develop a number of propositions regarding the critical success factors for EMR implementation [12].

ISO/IEC 27002: 2013 provides the guidelines for information security standards and management practices considering the information security risk environment of any organization. The area covers Information Technology, Security Techniques, and Information Security Management Systems of any IT System. The standard contains various security control clauses like information security policies; organization of information security; human resource security; asset management; access control; cryptography; physical and environmental security; operation security; communication security; system acquisition, development and maintenance; supplier relationships; information security incident management, etc.

1. Objective

The main aim and objective of this paper is to explore and analyze the present state of security and privacy of electronic patient records of hospital information systems. Also focus on policy at healthcare organization level on security and to develop a framework for information security in order to protect electronic health information system and patient records.

2. Research Questions

The research questions includes,

- What are the privacy and security issues of hospital information system setup specifically in super specialty tertiary care medical and research organization?
- How Electronic Patient Record (EPR) is protected currently?

3. Methodology

This section focuses on the aspects to find relevant sources where searches for particular studies will be done.

Sources should be selected in such a way that the searched materials are relevant to both security issues and challenges of the healthcare information system. Specific keywords related to above subjects will be used to possess search engines. The list of chosen sources is as following: IEEE Digital Library, ACM Digital Library, Science Direct, Scopus, other popular journals, and related books, etc.

Articles published between 2007 and 2015 have been taken into consideration for the purpose of searching in different databases related to the topic.

Three different sets of keywords ("Electronic Health Record and Security", "Electronic Medical Record and Security", "e-Health and Security") have been used to search through different databases. Searched articles were compared based on their titles. It was found that in spite of using different keywords most of the articles were duplicated and repeated. Therefore, Endnote software was used to avoid downloading duplicates. To identify more relevant articles, the abstracts were considered. From which 201 articles were selected. By going through the full text of papers, 62 articles were found to be more related for the purpose of this paper from which few articles are included.

4. Information Extraction

A. Love [11] in 2011 identified the current state of confidentiality, integrity, and availability standards that needs to be encountered to ensure that health care organizations are doing everything they can to protect patient health record. They also cover some of the security issues, including "confidentiality", "integrity", "availability", and "medical identity theft". As the result shows, healthcare organizations are doing everything they can within their budgets. It is very important to these organizations to implement all necessary polices and make sure everyone is following the protocols within the organization at all time. It is also important to ensure their vendors are following the same level of security as theirs.

Fernando and Dawson [4] in 2009 presented and discussed about the data collected through case study for a dissertation about medical professionals real life experiences on the electronic Health Information System (e-HIS) and also privacy and security experiences. The study was done on the basis of purposive sample of clinician, nursing staff, and other paramedical staff. The participants were interested and provided the information voluntarily. After the study it revealed that issues were related to poor training of staff and users, punitive threats, productivity challenges, and usability errors. Other reasons, include shared workplaces, outdated IT infrastructure, and constant interruption. Sometimes budgetary constraints are also responsible for security threats. Some preliminary suggestions and measures also presented for addressing the above mentioned issues.

C. Karunakaran, et al., [10] in 2012 identified the problem and resistances related to the usage of electronic healthcare records during collaborative information gathering process. This study was performed in the Emergency Department of a 500-bed training hospital. To collect required data, nonparticipant observations, and semi-structured interviews of patient care team members were carried out. A number of barriers were identified by using the analysis of collected data. The barriers appeared while using Electronic Medical Records during the investigations, include lack of collective afford, fear of deviations, and alert fatigues, clash of "technological frames". The finding of this study reveals an implication for designing Electronic Medical Record Systems that can facilitate and optimize better Hospital Information System.

D. Ana Ferreira et al., [5] in 2010 revealed that, the Grounded Theory (GT) can be used to involve healthcare professionals in the design and enhancement of access control policies for the users for accessing the Electronic Medical Record. The result of the study revealed that, the presented procedure can be used to involve health care professional and clinicians in making of access control policies to be applied to EMR system. The research showed that, the involvement of medical professionals along with the IT team is needed to frame an effective policy of for a hospital and health care organization. The study also reveals that, the Grounded Theory and Mixed Method can help to adapt access control system to healthcare professional and can also be used in similar research in information security domain.

Dong et al., [3] in 2012 show that, the research work has been made on privacy in e-health as a communication issue. Due to expected vast area of electronic health system in the near future and demand for interoperability of many sub systems privacy issues in healthcare has been taken. The authors' have researched on privacy needs for other than patients. The study also confirms that these two privacy challenges are necessary for securing e-health systems. The authors also suggested for adapting formal techniques which will help to understand and define these new privacy notions in more proper and accurate manner, and to develop an efficient verification framework for the same.

Noor Hafizah Hassan and Ismail [8] in 2012 investigated the current issues related to information security. It also identifies the key factors which influence the information security culture in healthcare informatics environment. A conceptual model was also proposed considering the factors influencing the information security. This also showed the various possible security issues specifically in healthcare IT which include threats in health information system, trust, information consent, security, policies in healthcare organization, various managerial issues, costs involved for adopting information security, and issues related to sharing of information.

G. Zayim, et al., [16] in 2011 expanded the evaluation methods that improve the understanding of people and organization influences related by concerning informatics applications development, and deployment. The findings of this research can be used as a guideline to enhance future system development processes and their connection with patient care.

Ghazvini and Shukur [6] in 2013 found out and analyzed the current status of electronic health systems security and privacy of patient health records. The main focus of this is on security at the policy level and developing a framework for health information security in order to protect electronic health record. Patient care practice involves collecting, synthesizing of information, and acting on it. It poses a great challenge to ongoing research and development for general frameworks and standards of healthcare information. Electronic Patient Record is one of the most important and valuable assets for any healthcare setup. After setting up the security system, an audit function is required to be organized. Audit is also needed in order for administrators and users to detect any unauthorized breach.

I. C. Derrick Huang et al., [9] in 2014 adopted a network-based approach to examine the economic aspects of information security for organizations. This study points to some future research directions and future studies can apply the mathematical modeling technique with other methodologies, such as qualitative case study to extend the usefulness and applicability of optimal information security investment for business benefits. Extension to this study would be to examine the economics of information security for the complete health information exchange as one scale free network.

5. Discussion

5.1 Security Issues

Every IT system including healthcare IT system has the security issues which need to be handled carefully. It should be managed proactively rather than through reactive mode. HIPAA guideline should be followed in case of every health IT system. HIPAA guidelines were passed to make health insurance more efficient and portable. Figure 1 shows the various aspects of HIPAA.

5.2 Security Challenges

There are various challenges which should be taken into consideration. Information stored in cloud may be vulnerable in respect of security. Viruses and malware may infect the system if proper security devices are not installed with the system. Handling of passwords is also an important aspect. Mobile devices used in the healthcare management system may also be vulnerable. Various healthcare specific security standards are shown in Figure 2.

This system offers several advantages, including healthcare practitioner input. But this is normally limited to practicing within the organization that hosts the health record system and those associated with. The first form is where patient data is stored on smartcards. Integrated systems are complex, but the complexity yields usability and flexibility [6]; One option is establishing a central system that gathers health information for all patients based on information that patients, and their providers have selected to be stored, and available [7]. A simple mistake by an individual within the organization may put the entire system in problem or risk such as:

- using a flash drive infected by a virus or containing a malware;
- accessing an email containing malware or a virus on one of the healthcare computers;
- allowing someone in unauthorized manner into an restricted area without knowing his intentions; and many more that need to be addressed clearly during staff trainings.

Any such organization specifically, healthcare organizations should ensure an implementation of necessary IT security policy along with electronics health policies. Encryption and password protection are the most commonly used techniques to guarantee the security and privacy of patient's health record system, but it will not be necessarily satisfactory in the case of bad systems or poorly chosen passwords [15]. Other way which can be used within a Local Area Network (LAN) is Media Access Control (MAC) address validation. Moreover, physical theft or indirect access could be avoided by data separation to prevent the data from being compromised. This could be obtained through the separation of health data from the identifying data stored in the form of registries [14]. Another technique is the separation of the encrypted data from the keys necessary to decrypt it [13]. In the separation of functions approach, different functional tasks are accomplished on separate systems, either physical or logical, for the purpose of isolating replaceable or exchangeable functions.

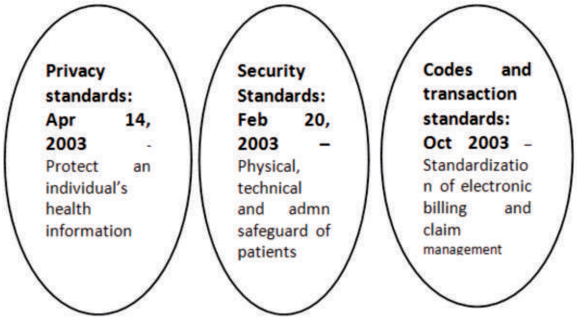
Privacy standards: Apr 14, 2003 - Protect an individual's health information
Security Standards: Feb 20, 2003 – Physical, technical and admn safeguard of patients
Codes and transaction standards: Oct 2003 – Standardization of electronic billing and claim management

Figure 1. HIPAA Guidelines

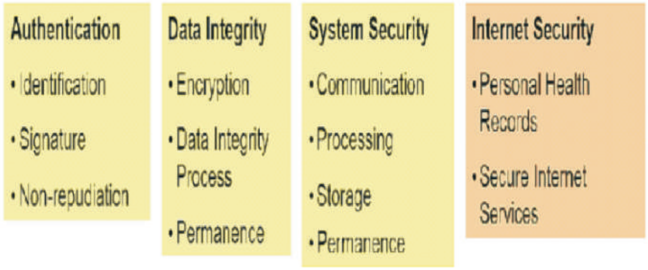

Figure 2. Healthcare-Specific Security Standards

Conclusion

Healthcare practice includes collecting data from various sources, and acting on information. It is therefore, a great challenge to ongoing research and development for general frameworks and standards for health informatics. Although, healthcare organizations are doing everything within their limitation and budget to protect Patient Health Records from any sorts of damage and misuse, there are some issues need to be considered. Organization could avoid this threat by conducting proper training within the employees and increasing human understanding. Once the security system has been established, an audit function is required. Auditing is a good practice to design and developany information system and also there should be some other measures to ensure complete data control and privacy. Date security and privacy applicability rules of hospital information system can be implemented with proper policies, framework, and cryptography techniques. Any health information system should comply with the mandatory health standards which will also help to maintain the privacy and security.

Recommendations and Future Work

There are continuous and ongoing researches on security issues on healthcare systems. Based on the findings and outcome of the research, it is important to enhance the security and privacy policy of health care organizations in order to protect electronic health records from being exposed to unauthorized access. One of the main threats to electronic health record security is the healthcare staff. Threats from employees can be divided into two categories: a) unauthorized access b) Lack of user training. By focusing on these factors health care can define every individual level of access to information they need within the organization as well as preventing redundant access to Electronic Patient Records. Sometimes users of the system do not understand the importance of the user ids and passwords allotted to them. It is time that healthcare organization should also take employee's awareness into consideration.

Acknowledgment

The authors gratefully acknowledge all the faculty, staff members, and persons involved for their valuable inputs and comments in studying the system.

References

[1]. Anderson, J. G. (2007). Social, ethical and legal barriers to e-health. *International Journal of Medical Informatics,* 76(5), 480-483.

[2]. Brady, J. W. (2011, January). Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers. In *System Sciences (HICSS), 2011 44th Hawaii International Conference on* (pp. 1-10). IEEE.

[3]. Dong, N., Jonker, H., & Pang, J. (2011, August). Challenges in eHealth: From Enabling to Enforcing Privacy. In *FHIES,* (pp. 195-206).

[4]. Fernando, J. I., & Dawson, L. L. (2009). The health information system security threat lifecycle: An informatics theory. *International Journal of Medical Informatics,* 78(12), 815-826.

[5]. Ferreira, A., Antunes, L., Chadwick, D., & Correia, R. (2010). Grounding information security in healthcare. *International Journal of Medical Informatics,* 79(4), 268-283.

[6]. Ghazvini, A., & Shukur, Z. (2013). Security challenges and success factors of electronic healthcare system. *Procedia Technology,* 11, 212-219.

[7]. Gunter, T. D., & Terry, N. P. (2005). The emergence of national electronic health record architectures in the United States and Australia: Models, costs, and questions. *Journal of Medical Internet Research,* 7(1), 87-94.

[8]. Hassan, N. H., & Ismail, Z. (2012). A conceptual model for investigating factors influencing information security culture in healthcare environment. *Procedia-Social and Behavioral Sciences,* 65, 1007-1012.

[9]. Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a Healthcare Information Exchange: An economic analysis. *Decision Support Systems,* 61, 1-11.

[10]. Karunakaran, A., Hee-Nam, Y., & Reddy, M. (2012, January). Investigating barriers to electronic medical record use during collaborative information seeking activities. In *Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium* (pp. 743-

748). ACM.

[11]. Love, V. D. (2011). IT Security Strategy: Is your Health Care Organization doing everything it can to protect Patient Information? *Journal of Health Care Compliance,* 13(6), 21-64.

[12]. MacKinnon, W., & Wasserman, M. (2009, January). Integrated electronic medical record systems: Critical success factors for implementation. In *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on* (pp. 1-10). IEEE.

[13]. Mandl, K. D., Simons, W. W., Crawford, W. C., & Abbett, J. M. (2007). Indivo: A personally controlled health record for health information exchange and communication. *BMC Medical Informatics and Decision Making,* 7(1), 25.

[14]. Ueckert, F., Goerz, M., Ataian, M., Tessmann, S., & Prokosch, H. U. (2003). Empowerment of patients and communication with health care professionals through an electronic health record. *International Journal of Medical Informatics,* 70(2), 99-108.

[15]. Wright, A., & Sittig, D. F. (2007). Encryption characteristics of two USB-based personal health record devices. *Journal of the American Medical Informatics Association,* 14(4), 397-399.

[16]. Zayim, N., Bozkurt, S., & Samur, M. K. (2011, October). Organizational issues in health informatics applications: Findings from a systematic review. In *Biomedical Engineering and Informatics (BMEI), 2011 4th International Conference on* (Vol. 4, pp. 1985-1988). IEEE.

ABOUT THE AUTHORS

Amal Krishna Sarkar, is a PhD student in the Department of Information Technology at Babasaheb Bhimrao Ambedkar University (a Central University), Lucknow, Uttar Pradesh, India. He completed his BE in Computer Science in the Department of Computer Science from Motilal Nehru Regional Engineering College, Allahabad. He completed his M.Tech. in Information Technology from KSO University, Mysore. His research interests are Healthcare Informatics and Health Information Security.

R. A. Khan is currently the Professor and Head of the Department of Information Technology at Babasaheb Bhimrao Ambedkar University, Lucknow, India.

C. M. Pandey is currently the Professor and Head of the Department of Biostatistics and Health Informatics at Sanjay Gandhi Postgraduate Institute of Medical Sciences, Lucknow, India.