RESEARCH PAPER | MEDICAL SCIENCE | Volume : 5 | Issue : 7 | July 2015 | ISSN - 2249-555X

The Security Challenges of Hospital Information System

KEYWORDS: Security challenges, Hospital information system, Information security, Electronic health record, computer security

Esmaeil Mehraeen	Dr. Reza Safdari	Dr. Marjan Ghazi Saeedi
Ph.D Student of Health Information Management, School of Paramedical, Tehran University of Medical Science, Tehran, Iran.	Associate Professor in Health Information Management, Department of Health Information Management, Tehran University of Medical Science, Tehran, Iran.	Assistant Professor in Health Information Management, Department of Health Information Management, Tehran University of Medical Science, Tehran, Iran.

ABSTRACT *Nowadays, information security and privacy in the healthcare area is an issue of rising importance. Security and privacy challenges of the e-health system need to be understood and considered more than before. One of the main threats to hospital information system security is the healthcare personnel. Threats from employees can be divided into three categories: a) Unauthorized access b) Lack of user training and c) Unwanted mistakes.*

The aim of this paper is to explore and analyze the security challenges in hospital information system (HIS). Main focus is on security at the policy level in order to protect electronic health record in hospital information system.

Introduction

Health care organizations around the world are demanding to satisfy customers, to compete with other organizations and to gain conventional score on the certifications. In recent years, these organizations, to provide services for their customers, have begun to use most advanced achievements of sciences. A hospital information system (HIS) is an element of health informatics that focuses mainly on the administrational needs of hospitals and also is one of the great achievements, which in recent years, using these systems has increased in healthcare centers [1]. These systems provide many benefits, some of which include: a reduction in costs, improved quality of care, the promotion of evidence-based medicine and record keeping and mobility. In order to achieve these benefits, HIS need to satisfy certain requirements in term of data completeness, resilience to failure, high availability, and the consistency of security policies [2].

The hospital information systems are vital for improving delivery of healthcare and the general support of stakeholders for its implementation. Although, in order to obtain a largely adopted and successful e-health system, there are still enormous challenges need to be solved [3]. However, because of its numerous challenges, the common usage of hospital information systems is still at a primary phase. Understanding the security as well as privacy issues are the key challenges in hospital information systems. Patients are obligated to share required information with their physicians. However, they may decline to disclose important information as expose of some information may result in social stigma and discrimination [4].

Based on other researches findings advanced countries require a lot of emphases on information security of medical organizations, whose governments also regulated many norms and rules to national medical organizations, such as the HIPAA of the United States and the NPFIT of England, mainly to enhance the service of medical quality, reduce the waste of medical resources, and prevent the occurrence of information security from impacting on medical services. In practical medical environment, there will be a transition period to fulfill the regulations and norms; and, enough time for establishment is also required [5].

Understanding the issues of privacy and security can be possible by using two interrelated factors (boundaries and motivated). So, the safety of hospital information systems in health care organizations is an issue that should be examined regularly [6]. Although, recent years have witnessed the design of standards and the promulgation of directives concerning security and privacy in information systems, more work should be done to adopt these regulations and to deploy secure healthcare systems [7].

Information security in the healthcare area is an issue of growing importance. The implementation of HIS, increased guideline, provider consolidation and the increasing need for information exchange between patients, providers and payers, all point towards the need for better information security in healthcare information systems. This is important to understand the security challenges of hospital information systems and factors can lead to enhance a successful security plan for HIS.

Material and methods

Research Aim

The aim of this paper is to explore and analyze the security challenges in healthcare information systems. Main focus is on security at the policy level in order to protect healthcare data in hospital information systems.

2.2 Research Question

What are the security challenges of hospital information system (HIS)?

How hospital information systems are protected currently?

The main purpose of this section is to find relevant sources where searches for particular studies will be executed. The selection of sources should be related to both security challenges and dimensions of the HIS. Selected keywords will be used to possess search engines. The list of chosen sources is as following: PubMed, Science Direct, EBSCO,

Volume : 5 | Issue : 7 | July 2015 | ISSN - 2249-555X

ProQuest, Web of Knowledge, Cochrane, Ovid, and Scopus (Figure 1).

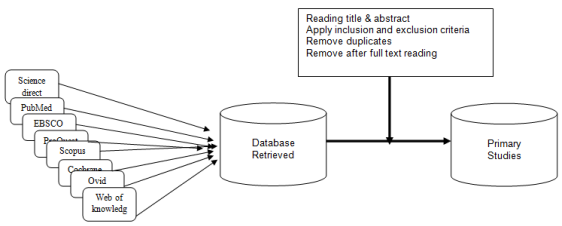

Figure 1: Study source selection

Results

All articles from 2000 till 2014 have been taken into account for the purpose of searching in different databases. Three different sets of keywords (Information security, Computer security, Hospital information systems security, Information security management, Information systems security, Information security strategy, Healthcare information systems security, Hospital information systems and information security, Hospital information systems and security) have been used to search through variant databases. Appeared articles were compared based on their titles. It was noticeable that, even though, different keywords have been used, most of the articles were duplicated. On the other hand, Endnote software helped to avoid downloading duplicates. To identify more relevant articles, the abstracts were considered by which 210 articles were selected. By going through the full text of papers, 52 articles were found to be more related to the purpose of this paper from which 48 articles are included. Moreover, from all the articles referenced in this paper, 19 articles are used for the purpose of analysis (Table 1).

Table 1: Search result from different databases

Year Published	2000-2014				
Research Question	Total Reference Retrieved	Total Abstract Screened	Total Full-Text Screened	Final Included Papers	Number of Analyzed Articles
RQ1	415	132	35	33	11
RQ2	250	78	17	15	8
Total	665	210	52	48	19

4. Discussion

4.1 Research Question 1

Health records are particularly sensitive to each of the so called CIA (Confidentiality, Integrity, and Availability) aspects. Health records are obviously confidential, because they may expose the health conditions of a patient to unauthorized people. Integrity is also very important: what happens if inaccurate data lead to a wrong clinical treatment? Talking about availability, no one would like that a power supply failure causes the interruption of the wide area network linking the surgery rooms with the external facility where a doctor is performing Tele-surgery [8].

Proper configuration of security technologies is critical to balance the needs for access and protection of information in healthcare systems. The common practice of using a layered security architecture that has multiple technologies amplifies the need for proper configuration because the configuration decision about one security technology has ramifications for the configuration decisions about others [9]. There has been very little activity in policy development involving the numerous significant privacy issues raised by a shift from a largely disconnected, paper-based health record system to one that is integrated and electronic [10]. Moreover, the advances in Information and Communications Technologies have led to a situation in which computerized patients' health data are confronting new security and privacy threats [11]. The three fundamental security goals in HIS are confidentiality, integrity and availability (CIA). The protection and security of personal information is critical in the health sector, and it is thus necessary to ensure the CIA of personal health information in HIS [12].

Further the advantage of the HIS designs, there are barriers that reduce their usage. Complexity, access, and data bases are features that define the operational characteristic of the three designs and threats, security, and privacy define the challenges to acceptance of HIS designs. Understanding of these features and characteristics enables clinics to compare HIS designs and impalement the most proper design for their usage. Human error is also one of the most challenging concerns that need extra attention. By increasing human accepting in the organizations, human errors could be reduced. Healthcare employees need to be aware of their important role to protect organization's vital information and to avoid imperiling the system by a recruit mistake. Healthcare organization is responsible to conduct sequences of appropriate trainings for their personnel to increase their level of understanding from the system. A simple mistake by an individual within the organization may put the entire system in risk such as: a) carrying a flash drive from infected by a virus or containing a malware; b) opening an email containing malware or a virus using on one of the healthcare computer; c) allowing someone unauthorized into an regulated area without knowing his intentions; and many more that need to be attention clearly during employees trainings.

4.2 Research Question 2

This is essential for organizations to ensure an implementation of necessary security policies. It is also important that everyone within an organization complies with those policies. All the stakeholders involved in health information exchange, such as vendors, patients, doctors, and medical assistants should follow the same level of security because they all play important roles that affect care practices.

An assessment role is a necessity as soon as the founding of the security system. Assessment is needed so administrators and users are able to review the list of accesses to the HIS data. This way any illegal or unauthorized break can be easily detected and acted upon [13]. Another important matter on privacy concerns is that the patients are the legal owners of their data that exist within, or can be accessed by a HIS system. In such a system the data owner has the right to authorize or decline an access to any or all of the data. This may include any or all individuals, even the caregivers [4].

Password and encryption protection are the best ways to guarantee the security and privacy of HIS, but it will not be necessarily suitable in the case of bad systems or poorly chosen passwords [14]. Furthermore, 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 [15]. Another technique is the separation of the encrypted data from the keys necessary to decrypt it [16]. In the separation of functions approach, different functional tasks are accomplished on separate systems, either physical or logical, for

Volume : 5 | Issue : 7 | July 2015 | ISSN - 2249-555X

the purpose of isolating replaceable or exchangeable functions [4].

5. Conclusion

The healthcare industry involves collecting, processing, saving, acting on and sharing information and therefore poses a great challenge to ongoing research and development for general outlines and standards. A HIS is one of the most important properties for a healthcare organization. HIS allow structured healthcare data to be shared between authorized healthcare team in order to improve the quality of healthcare delivery and to achieve enormous savings. In these systems, privacy and security concerns are extremely important, since the patient may encounter serious problems if sensitive information is disclosed.

Nowadays, due to the development of health information systems in health care centers, using equipment, software, and applications of these systems has also increased. Use of hospital information system is one concern in the health sector because of growing challenges of health information management processes and also due to the significant diversity and innovation in the supply system [17]. Human error is the most challenging issue that needs to be taking into consideration. It may happen in level of access within the organization with a dramatic effect on the system. Organization could avoid this threat by leading proper training and increasing human understanding. Once the security system has been established, an audit and assessment functions are required. Audit is needed in order for administrators and users to detect any illegal or unauthorized breach [13]. Consistent evaluation of system with formal methods offers strong indications and suggestions about the financial influences and its impact on increasing efficiency, quality and security [18].

5.1 Recommendations

We have perceived that it is important to enhance the policy of healthcare organizations in order to protect patient information in HIS from being exposed to unauthorized access. One of the main threats to hospital information system security is the healthcare personnel. Threats from employees can be divided into three categories: a) Unauthorized access b) Lack of user training and c) Unwanted mistakes. By focusing on these factors health cares can define every individual level of access to information they need within the organization as well as preventing redundant access to HIS. It is logical to use an effective encryption system that is easy to use by healthcare staff, is easily extensible to HIS, and have a reduced number of keys held by each party. It is time that healthcare authorities take employee's awareness into consideration. They need to ensure all recruits are being inducted in HIS information security policy and educational programs which address issues of privacy and security for healthcare professionals and health organizations should be developed.

6. Highlights

Human error is the most challenging issue that needs to be taking into consideration.

Audit and assessment functions are required once the security system has been established.

Policy making in healthcare organizations in order to protect patient information in HIS from being exposed to unauthorized access is mandatory.

7. Acknowledgments

This study was funded and supported by Tehran University of Medical Sciences (TUMS); Grant no. 523.

REFERENCE

1. Mehraeen E, Ahmadi M, Mehdipour Y, Noori T. Evaluation of hospital information systems in selected hospitals of Iran. International Journal of Advanced Information Technology 2014; 4(5): 1-5. | 2. Allard T, Anciaux N, Bouganim L, Guo Y, Folgoc LL, Nguyen B, et al. Secure personal data servers: a vision paper. PVLDB 2010; 3(1–2):25–35. | 3. Srur BL, Drew S. Challenges in designing a successful e-health system for Australia. International Symposium on Information Technology in Medicine and Education, Griffith University, Australia. 2012. | 4. Daglish D, Archer N. Electronic personal health record system: a brief review of privacy, security, and architectural issues. Word Congress on Privacy, Security, Trust and the Management of e-Business, 2009. DeGroote School of Business. McMaster University. | 5. Liu CH, Chung YF, Chen TS, Wang SD. The enhancement of security in healthcare information systems. J Med Syst 2012; 36:1673–168. | 6. Zakaria N, Stanton J, Stam K. Exploring security and privacy issues in hospital information system: an information boundary theory perspective. J Am Med Inform Assoc 2003; 17(6): 1059. | 7. Aleman JLF, Senor IC, Lozoya PAO, Toval A. Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics 2013; (46): 541-562. | 8. Cavalli E, Mattasoglio A, Pinciroli F, Spaggiari P. Information security concepts and practices: the case of a provincial multi-specialty hospital. Int J Med Inform 2004; 73(3):297-303. | 9. Cavusoglu H, Raghunathan S. Configuration of and Interaction between information security technologies: The case of firewalls and intrusion detection systems. Information Systems Research 2009; 2(2): 198–217. | 10. Rothstein MA. Health privacy in the electronic age. J Leg Med 2007;28(4):487–501. | 11. Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. Security requirements and solutions in electronic health records: lessons learned from a comparative study. J Med Syst 2010;34(4):629–42. | 12. Haas S, Wohlgemuth S, Echizen I, Sonehara N, Muller N. Aspects of privacy for electronic health records. Int J Med Inform 2011;80(2):e26–31. | 13. Canada Health Infoway (CHI). 2007. White Paper on Information Governance of the Interoperable Electronic Health Record (EHR). Available online: http://www2.infowayinforoute.ca/Documents/Information%20Governance%20Paper%20Final_20070328_EN.pdf (Jan 8 2009)," Canada Health Infoway, Montreal. | 14. Wright A, Sittig DF. Encryption characteristics of two USB-based personal health record devices. Journal of the American Medical Informatics Association, 2007; 14:397-399. | 15. Ueckert F, Goerz M, Ataian M, Tessmann S, Prokosch HU. Empowerment of patients and communication with health care professionals through an electronic health record. International Journal of Medical Informatics, 2003; 70:99-108. | 16. Mandl KD, Simons WW, Crawford WCR, Abbett JM. Indivo: a personally controlled health record for health information exchange and communication. BMC Medical Informatics and Decision Making, 2007;7:1-10. | 17. Mehraeen E, Ayatollahi H, Ahmadi M. A study of information security in hospital information systems. Health Inf Manage 2014; 10(6):788. | 18. MacKinnon W, Wasserman M. Integrated electronic medical record system: critical success Factors for implementation. Proceeding of the 42nd Hawaii International Conference on System Sciences, 2009. Clarkson University. |