The 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013)

Security Challenges and Success Factors of Electronic Healthcare System

Arash Ghazvini*, Zarina Shukur

Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor Darul Ehsan, Malaysia

Abstract

Potential benefits of the e-health system do not ignore the challenges that prevent the system from being fairly used. Security and privacy challenges of the e-health system need to be understood and resolved. The aim of this paper is to explore and analyze the current state of e-health systems security and privacy of patient records. Main focus is on security at the policy level in order to protect electronic patient record.

© 2013 The Authors. Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
Selection and peer-review under responsibility of the Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia.

Keywords: EHR, EHS, Security, Privacy

1. Introduction

The potential advantages of the e-health system have been considered over recent decades. However, because of its several challenges, the widespread usage of e-health system is still at an early stage. Understanding the security as well as privacy issues are the key challenges in e-health system. The principle that govern the patient–physician relationship is view as privacy. Patients are obligated to share required information with their physicians. However, they may decline to reveal important information as disclosure of some information may result in social stigma and discrimination [4].

This is important to understand how far electronic health records are protected and what factors can lead to enhance a successful e-health system. Over time, EHR accumulates personal information that is significant to one’s life and social status.

* Corresponding author. Tel.: +60-19-613-4737.
E-mail address: arash@fism.ukm.my
2. Research Aim

The aim of this paper is to explore and analyze the current state of e-health systems security and privacy of patient records. Main focus is on security at the policy level and developing a framework for information security in order to protect electronic patient record.

3. Research Question

- What are the Privacy and security Issues of electronic healthcare system (EHS)?
- How electronic health record (EHR) is protected currently?

4. Methodology

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 and issues of the EHS. Selected keywords will be used to possess search engines. The list of chosen sources is as following: IEEE digital library, ACM digital library, Science Direct and Scopus (Fig 1).

All articles from 2001 till 2012 have been taken into account for the purpose of searching in different databases. 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 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. Therefore, Endnote software helped to avoid downloading duplicates. To identify more relevant articles, the abstracts were considered by which 201 articles were selected. By going through the full text of papers, 69 articles were found to be more related to the purpose of this paper from which 46 articles are included. Moreover, from all the articles referenced in this paper, 12 articles are used for the purpose of analysis (Table 1).

5. Information Extraction

A. Love. 2011. IT Security Strategy: Is Your Health Care Organization Doing Everything It Can to Protect Patient Information?. [13]

The aim of this article is to identify 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 PHR. 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 vital to these organizations to implement all necessary policies and to 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.

B. Fontaine, et al. 2010. Systematic Review of Health Information Exchange in Primary Care Practices. [6]

A systematic review has been conducted by the authors of this article from January 1990 until September 2008. The objective of this study was to distinguish peer reviewed and non-peer reviewed publications from variant website and databases. Each publication has been abstracted to identify main issues. Stakeholder involved in health information exchange plays an important role and it influences the benefits, barriers, and overall value to primary care practices. As health information exchange initiatives and pilot plans increase, they need to be properly analyzed with research methods. A consist analysis offers strong indications and suggestions about the financial influences and its great impact on increasing actual efficiency, quality, and safety.
The goal of this research study is to identify the barriers related to the usage of electronic medical records during collaborative information seeking activities. Authors conducted qualitative research approaches to point out how individuals’ entities within patient care teams employ EMRs during CIS. It also reflects the challenges they have to deal with as they encounter in the process. This study has been done 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 through the analysis of collected data. These barriers, that appear while using EMRs during CIS, include lack of collective affordances, fear of deviations and alert fatigues, clash of "technological frames". The finding of this study underlines an implication for designing EMR systems that can facilitate and optimize better CIS.

This paper introduces a goal centric and policy driven framework for deriving security and privacy risk mitigation strategies in ubiquitous health information interchange. The main focus is on scenario analysis and goal oriented techniques to model security and privacy objectives, threats, and mitigation strategies in the form of safeguards or countermeasures are used. While introducing the idea of purpose driven security policies based on sensitivity Meta tags is demonstrated, the authors found that traditional solutions are insufficient. It also shows administrative safeguards are refined into intermediate specifications that can be analyzed more systematically.

Due to a vast distribution of e-health system in the near future, this paper studies privacy in e-health as a communication issue, which demand for interoperability of many sub systems. Further, the authors research on privacy needs for others than patients. Two main privacy challenges in e-health are highlighted in this study, namely enforced privacy and privacy in the presence of others. The study confirms that the two identified privacy challenges are necessary for securing e-health systems. The Authors also recommend that in order to enhance a better understanding of these challenges, more researches need to be conducted. They suggest to adapt formal techniques that help to understand and define these new privacy notions in a more accurate manner, and to develop an efficient verification framework.

This research provides an introduction to Personally Controlled Electronic Health Records (PCEHRs) in Australia by studying the relevant concepts that have been acknowledged in the literature of technology acceptance models and Information Systems success models. Authors present a latest review of the challenges occur while implementing PCEHRs in Australia. The study indicates that these 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.

The concern of this paper is to expand 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.
Affecting factors may differ because they are the result of different settings, such as different type of organizations (clinic, hospital, or doctor office), different cities, and different countries. Since doctors are the key users of an e-health system, they were pointed as the main targets for interview in this research. Although, it is worth noting that there are also other people who has access to a system with different needs and objectives such as nurses, medical assistants, administrations and etc. It was found from the interview that the privacy of the system, user interface, data quality, information quality, and flexibility are the key factors of “Perceived ease of use”. Further, the survey highlighted that functionality and job relevance, quality support, quality of care, and sharing are the key sub-factors of “Perceived Usefulness”.

I. MacKinnon & Wasserman. 2009. Integrated Electronic Medical Record System: Critical Success Factors for Implementation. [14]

In this paper EMR was considered as a type of enterprise resource planning (ERP) system. The authors investigate on the issues of EMR implementation through an empirical research from both ERP literatures and the healthcare information systems. Based on structured interviews with health care professionals, they proposed a theoretical model and propositions. The paper highlighted a number of important success factors, namely planning, consultants, process redesign, project management and the need for a project champion.

J. Daglish & Archer. 2009. Electronic Personal Health Record System: A Brief Review of Privacy, Security, and Architectural Issues. [4]

The focus of this paper is on the design and architectural problems in PHR system. More specifically, the authors looked at privacy and security aspects because they believe that an acceptance of PHR by public requires a careful analysis of privacy and security issues. Daglish and Archer divided PHR system architecture into four categories: i) Tethered PHRs ii) Standalone PHRs iii) Integrated PHRs iv) Other PHR models. Further, a system was proposed and developed by authors after an analysis of clinical consultation workflow and systematic review of other health information system.

K. Ghani & Wen. 2011. Design of Flexible Pervasive Electronic Health Record (PEHR). [8]

In the arena of Electronic Health Record, availability of medical history is very important. Therefore, storage devices such as mobile phone, USB, laptop, and etc. provide a flexible access to patient medical record. Thus, the aim of this paper is to propose a seamless access to patient HER. This system provides an immediate access to patient medical history which can lead to more accurate and efficient treatments.

L. Borovicka. 2008. DMIS: The Design and Prototype of a Future Clinical e-Health. [1]

This article investigated the very early stages of a project that attempts to develop solutions for improving medical care through a development of prototype and applying related mechanisms in order to reduce interaction time and enable an integration of new information sources. Thus, the objective of this article was to find a solution for clinical diagnosis process which intends to boost system use by providing alternative information for decision making.

6. Discussion

6.1. Research Question 1

In an age of data snooping and identity theft, it is not surprising that there is an apprehension for security and privacy in PHRs. There are three type of common PHRs including Tethered PHRs, Standalone PHRs, and Integrated PHRs [4]. A tethered PHR is a system that is accessible by the patient and in some way it is connected to an organization’s system. Tethered PHR systems offer several advantages, including healthcare practitioner input. However, this is normally limited to practicing within the organization that hosts the PHR and those associated with.

There are two possible forms of standalone PHR. The first form is where patient data is stored on smartcards
PHRs. There are some portable media devices and smartcard is the one that is supported by software. Smartcard can be accessed by computer in order to view, modify, or organize the data. In the second form standalone PHR, consolidator PHRs are commonly in the form of centralized Internet portals. In this form the patient can gathers data from other sources and which also can enter desired data. The integrated PHR is system driven, and collects and presents patient data from several sources into a single view. Integrated systems are complex, but the complexity yields usability and flexibility [43]. 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 [44].

Besides the benefit of the PHR architectures, there are limitations that diminish their usage. Complexity, access, and data sources are attributes that define the operational characteristic of the three architectures and risks, security, and privacy define the barriers to acceptance of PHR architectures. Understanding of these attributes and characteristics enables clinics to compare PHR architectures and implement the most appropriate architecture for their usage.

Furthermore, human error is also one of the most challenging issues that needs extra attention. By increasing human understanding in the organizations, human errors could be reduced. Healthcare staffs need to be aware of their important role to protect organization’s vital information and to avoid compromising the system by a rookie mistake. Healthcare organization is responsible to conduct series of proper trainings for their employees to increase their level of understanding from the system. A simple mistake by an individual within the organization may put the entire system in jeopardy such as: a) bringing 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) letting someone unauthorized into an restricted area without knowing his intentions; and many more that need to be addressed clearly during staff trainings.

6.2. Research Question 2

This is essential for organizations to ensure an implementation of necessary e-health 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.

Encryption and password protection are the finest ways to guarantee the security and privacy of PHRs, but it will not be necessarily satisfactory in the case of bad systems or poorly chosen passwords [36]. 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 [38]. Another technique is the separation of the encrypted data from the keys necessary to decrypt it [39]. 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 [4].

An audit function is a necessity as soon as the establishment of the security system. Audit is needed so administrators and users are able to review the list of accesses to the PHR data. This way any illegal or unauthorized breach can be easily detected and acted upon [41]. Another important note on privacy concerns is that the patients are the rightful owners of their data that reside within, or can be accessed by, a PHR 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].

7. Conclusion

Health care practice involves collecting, synthesizing, and acting on information and therefore poses a great challenge to ongoing research and development for general frameworks and standards. EPR is one of the most valuable assets for a healthcare organization. Even though they are doing everything they can within their budget to protect PHRs from any sorts of damage, there are some issues to be take into account as they have been discussed in the previous sections. 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 conducting proper training and increasing human understanding. Once the security system has been established, an audit function is required. Audit is needed in order for administrators and users to detect any illegal or unauthorized breach [4][41]. 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 [14].

8. Recommendations and Future Work

There is an ongoing research on security issues on healthcare systems. Based on our findings, it is important to enhance the policy of healthcare 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 cares can define every individual level of access to information they need within the organization as well as preventing redundant access to EPRs. It is time that healthcare authorities take employee’s awareness into consideration. They need to ensure all recruits are being inducted in EPR information security policy and employee’s regular basis trainings on security policy are implemented.

Reference

[1] Borovicka M. DMIS: Design and Prototype of a Future Clinical e-Health. Proceeding of MoMM. University of Innsbruck. Austria; 2008.
[2] Brady JW. Securing Health Care: Assessing Factors that Affect HIPAA Security Compliance in Academic Medical Centers. Proceeding of the 44th Hawaii International Conference on System Sciences, Nova Southeastern University; 2011.
[3] Coveney HD. Formal Structure for Specifying the Content and Quality of the Electronic Health Record. 11th IEEE International Requirement Engineering Conference, Canada; 2003.
[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] Dong N, Jonker H, Fang J. Challenges in e-Health: From Enabling to Enforcing Privacy. International Symposium on Foundations of Health Information Engineering and Systems (FHIES), Computer Science, 2012; 7151, p 195-206.
[6] Fontaine P, Ross SE, Zink T, Schilling LM. Systematic Review of Health Information Exchange in Primary Care Practices. The Journal of the American Board of Family Medicine, 2010.
[7] Fragidis LL, Chatzoglou PD. The Use of Electronic Health Record in Greece: Current Status. 11th IEEE International Conference on Computer and Information TechnologyDemocritus University of Thrace, Greece, 2011.
[8] Ghani MKA, Wen LC. The Design of Flexible Pervasive Electronic Health Record (PEHR). IEEE Colloquium on Humanities, Science and Engineering Research (CHSER) University Teknikal Malaysia Melaka, Malaysia; 2011.
[9] Han S. A Framework of Authentication and Authorization for E-Health Services. In Proceedings of the 3rd ACM workshop on Secure web services (SWS ’06). ACM, New York, NY, USA, 2006;105-106.
[10] Karunakaran A, Young HN, Madhu R. Investigating Barriers to Electronic Medical Record Use During Collaborative Information Seeking Activities. The 2nd ACM SIGHIT International Health Informatics Symposium, 2012, p. 743-748.
[11] Kashfi A. The Intersection of Clinical Decision Support and Electronic Health Record: A Literature Review. IEEE Proceeding of the Federated Conference on Computer Science and Information System.Chamlers University of Technology. 2011.
[12] Kok OM, Basoglu N, Daim, T. Exploring the Success Factors of Electronic Health Record System Adoption. Proceedings of PICMET ’12: Technology Management for Emerging Technologies. Bogazici University. Turkey; 2012.
[13] Love DL. IT Security Strategy: Is your Health Care Organization Doing Everything It Can to Protect Patient Information? Journal of Health Care Compliance, 2011.
[14] 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.
[15] Parker ME, Pandya AS. Assuring Nursing’s Voice in the Electronic Health Record. Florida Atlantic University; 2007.
[16] Suru 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.
[17] J. Weber-Jahnke H, Obry O. Protecting privacy during peer-to-peer exchange of medical documents. Information System Frontiers, 2012; 14:87–104.
[18] Zayim N, Bozkurt S. Organizational Issues in Health Informatics Applications: Finding from a systematic Review. 4th IEEE International Conference on Biomedical Engineering and Informatics (BMEI), Akdeniz University, Turkey. 2011.
[19] Oladimej A, Chong L. Managing Security and Privacy in Ubiquitous e-Health Information Interchange. The 5th International Conference on Ubiquitous Information Management and Communication, Article No. 26. 2011.
[20] Weber-Jahnke JH. & Mason-Bialek, F. The Safety of Electronic Medical Record (EMR) Systems. SIGHIT Record, 2011;1(2).
[21] Gostin LO. Privacy and security of personal information in a new health care system. The Journal of the American Medical Association, 2003;270: 270–274.
[22] Janiczewski, L. Development of Information Security Baselines for Healthcare Information System in New Zealand. Computer and Security, 2003;21: 172-192.
[23] Rigby M. Verifying quality and safety in health informatics services. Information in Practice, 2001;323:552-556.
[24] Sucurovic S. Implementing security in a distributed web-based EHCR. International Journal of Medical Informatics, 2007;76:491-496.
[25] Deng M. Privacy Preserving Content Protection. PHD thesis submitted to Katholieke Universality, England; 2010.
[26] Coleman A. Developing an e-Health Framework through Electronic Healthcare Readiness Assessment PHD thesis submitted to Nelson Mandela Metropolitan University; 2010.
[27] Meingast M, Roosta T, Sastry S. Security and Privacy Issues with Health Care Information Technology. Proceedings of the 28th IEEE,
[28] Appari A, Johnson ME. Information security and privacy in healthcare: current state of research. Int. J. Internet and Enterprise Management, 2010; 6(4).

[29] Applebaum PS. Privacy in psychiatric treatment: threats and response. American Journal of Psychiatry, 2002;159:1809–1818.

[30] Sankar P, Moran S, Merz JF, Jones NL. Patient perspectives on medical confidentiality: a review of the literature. Journal of General Internal Medicine, 2003;18:659–669.

[31] Mercuri RT. The HIPAA-potamus in health care data security. Communications of the ACM, 2004;47(7):25–28.

[32] Chan D. Welcome to MyOSCAR - Your Personally Controlled Health Connection. Available online: http://www.stonechurchclinic.ca/myoscar. Hamilton, Ontario: Stone church Family Health Centre, 2008.

[33] Intersystem. 2008. The U.S. Department of Veterans Affairs uses Intersystem Ensemble to integrate 130 systems and improve patient care. Available online: http://www.intersystems.com/casestudies/ensemble/usdva.pdf. Intersystem Ensemble Case Study.

[34] Gesundheitskarte. 2008. German electronic healthcare. Available online: http://www.healthcareitnews.eu/index.php?Itemid=&option=com_search&searchword=gesundheitskarte (Jan 7 2009). Europe Healthcare IT News.

[35] Anonymous. 2008. Microsoft HealthVault scores big win: Pilot with Kaiser. Available online: http://www.networkworld.com/community/node/28560 (Jan 7 2009),” in Network World.

[36] 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.

[37] Simons WW, Mandl KD, Kohane I. The PING Personally Controlled Electronic Medical Record System: Technical Architecture. Journal of the American Medical Informatics Association, 2005;12: 47-54.

[38] Ueckert F, Goerz M, Atajan 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.

[39] 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.

[40] Sax U, Kohane I, Mandl KD. Wireless Technology Infrastructures for Authentication of Patients: PKI that Rings. Journal of the American Medical Informatics Association, 2005;12:263-268.

[41] 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.

[42] Dorr D, Bonner LM, Cohen AN, Shohi RS, Perrin R, Chaney E, Young AS. Informatics Systems to Promote Improved Care for Chronic Illness: A Literature Review. Journal of the American Medical Informatics Association, 2007;14:156-163.

[43] Tang PC, Ash JS, Bates DW, Overhage JM, Sands DZ. Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption,” Journal of the American Medical Informatics Association, 2006;13:121-126.

[44] Gunter DT, Terry PN. The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions,” J Med Internet Res, 2005;7:e3.

[45] Valerius JD. The Electronic Health Record: What Every Information Manager Should Know. Information Management Journal. 2007; 41(1):56-59.

[46] Brown B. Privacy Provisions of the American Recovery and Reinvestment Act. Journal of Healthcare Compliance, 2009;37-73.
Appendix A.

Fig. 1. Study source selection

Table 1. Search result from different databases

| Research Question | 2001 - 2012 | Year Published |
|-------------------|-------------|----------------|
|                   | Total       | Total          | Total Full- | Final   | Number |
|                   | Reference   | Abstract       | Text Screened| Included | Analyzed |
| RQ1               | 414         | 131            | 48          | 32      | 7       |
| RQ2               | 204         | 70             | 21          | 14      | 5       |
| Total             | 618         | 201            | 69          | 46      | 12      |