Journal of Engineering and Applied Sciences 13 (17): 7271-7276, 2018
ISSN: 1816-949X

Security-Based Framework for Electronic Health Records (EHRS) Development: A Preliminary Review

Zuraimeen Othman, Nsafie and Khaldoon Aliway
Center for Software Technology and Management (SOFTAM),
Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia,
43600 Bangi, Malaysia

Abstract: Electronic Health Records (EHRs) created by health care organizations that provide health care services (clinics and hospitals). Electronic health records are required due to the growth of information exchange among the healthcare providers. Although, the EHR implementation is expanding in worldwide, research has revealed that security is so critical that major deployments require security to be part of the solution besides functionality, interoperability and utility. This study therefore analyzed security as an integral factor in electronic health records development. By using the content analysis method, five security standards and model were qualitatively analyzed and reviewed. The analysis include the Personal Data Protection Act 2010 ("Act PDP"), the Health Insurance Portability and Accountability Act (HIPAA), Information Security Management System (ISMS), Confidentiality, Integrity and Availability (CIA) Triad Model and also Malaysia IHE (MyHIX). The findings from the reviews were combined and used to form the recommended framework. It is found that, even though there is a framework developed by earlier researchers but it seems to be more on general framework and to the best knowledge of the searchers, no one has focused on the security and privacy of data in particular. This framework can be used as a guide by health care organizations or government agencies to produce an action plan for the development of the electronic health records system security and comply with higher standards. On the whole, this should lead to better patient health outcomes and improve safety in electronic health records.

Key words: Electronic, health records, patient privacy, end to end security, control health, information exchange

INTRODUCTION

For the purposes of this study, operationally EHR refers to any health, clinical or medical records stored electronically or digitally and with regard to patient care. EHR has been widely accepted, implemented and used. It has also been recognized as an expensive capital investment accenture in an industry report (Anonymous, 2010) for the period from 2010-2013 predicted that the adoption of EHR would continue to see a substantial increase globally but at different rates in various regions. Digital-based healthcare solutions have bought about a transformation in the health care sector, enabling it to be much more efficient, more cost-effective and more effective in terms of quality healthcare delivery (Liu and Park, 2011). Electronic health records have great potential to improve healthcare by facilitating fast and accurate data transmission, standardizing medical processes, enabling decision support and allowing real-time medical error prevention, to name the major benefits. The main drivers of implementing EHR are the sharing and dissemination of healthcare information and data technologies that make patient records available to multiple interested parties. Due to the sensitivity of patient health records, security is a priority in the electronic health records system because it is a part of the solution together with its functional role as well as offering interoperability and utility (Anonymous, 2010). Also because the reach of and access to EHR is not limited to only the local and regional context but is also global in nature, securing the confidentiality of the EHR information poses a challenge to software designers in terms of the security architecture of EHR solutions.

To protect the confidentiality of patient's health records has long been emphasized in previous research. Past studies on information privacy have been linked to concerns about privacy but the research outcomes have mostly paid attention the organizational level and

Corresponding Author: Zuraimeen Othman, Center for Software Technology and Management (SOFTAM),
Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia,
43600 Bangi, Malaysia

insignificant focus on the association between antecedents and privacy concerns (Blumenthal, 2011). With the rapid and extensive growth of Healthcare Information System (HIS), concerns about the security of private information have been voiced by both researchers and healthcare personnel. Symantec in internet security threat report (2013), reported that organizations in the healthcare sector still constitute the highest rate of known data breaches by industry (Smith *et al*., 2011). There have been more security threats in the past few years and in excess of 1.5 million names linked to EHRs have been exposed in relation to data breaches (Smith *et al*., 2011). Ponemon Institute (Symantec, 2012) recently reported that the majority of healthcare organizations have a problem in dealing with privacy and data security risks as a result of inadequate technologies, resources and trained personnel.

This study seeks to investigate the availability of security models for EHR for the purpose of understandin their characteristics. Besides that it will identify the gaps that further studies could bridge. The following section presents works associated with security framework for EHR. It is then followed by the metodology employed in the current work. Later, the findings will be presented and discussed followed by the conclusion which will provide a concise summary of the current research and suggest future research options.

Literature review: Moving forward from the adoption of EHRs, many countries are now looking at possibilities and potential of converting patient records onto the digital platform which would imply also the computerization of health information for accessibility at the right time in the right place and in usable format. This would mean the use of systems that are interoperable, patient-centred and are user-friendly systems as shown by Anonymous (2012).

To be interoperable means to be able to exchange health information and enjoy the social benefits that are promised by the adoption of EHRs (Kellermann and Jones, 2013). Information exchange needs the transmission of data by means of networking technology, in addition to the crucial role of development and promotion of health standards (Brailer, 2005). Maximum benefits can be enjoyed if there is full implementation of Health Information Exchange (HIE) (Kuperman *et al*., 2010). HIE has attracted much many in the academia and in government (Walker *et al.* 2005). Despite the model of exchange, the notion of sharing patient data among multiple parties gives rise to fears concerning the privacy of patients and security.

EHR background information

EHR: Electronic Health Record (EHR) This system offers a total and precise summary of an individuaj patient's medical record. According to Kuperman (2011) EHR is a longitudinal electronic record of patient health information produced by one or more meetings in any care delivery setting. This comprises information such as demographic details of patients, notes of patient's progress, problematic issue, medication details, vital signs, and medical history, immunizations, laboratory tests data and radiology reports. The EHR is capable of generating a comprehensive dossier of a patient and also to facilitate evidence-based decision support, quality management and outcomes reporting.

Health Information Exchange (HIE): However, even though it is obvious that they are many worthwhile and important advantages, EHRs have one significant drawback that persists. The health personnel using EHRs comprise a heterogeneous mix and individually they all have their own sets of technologies and policies and this hampers interoperability. Information exchange across provider boundaries can be problematic. While such exchange can be achieved, system incompatibility between different system formats and coding can still occur and will nullify the exchange. Such a scenario is akin to a fragmentation issue and causes data fragmentation across several sectors. Consequently, the benefits of the global context of HI are lost. This fragmentation is a fundamental factor that contributes to higher expenditure and impaired general performance of the macro healthcare system (Garets and Davis, 2006). The negative outcomes are absence of responsibility, medical errors, wastage and unnecessary duplications.

Benefits of HIE: Safety healthcare will be safe if important information, like allergies and ongoing medications are available prior to the prescription of new interventions (Benli *et al*., 2012). An emergency care can be especially, safe if HI is exchanged as shown by Payne *et al.* (2010). According to Shapiro *et al.* (2006) and Kaelber and Bates (2007) a maximum of 18% of patient safety mistakes and as high as 70% of undesirable drug events can be removed if the correct information for the right patient is obtainable when it is needed. HIE can enable this situation.

Patient perception: It is important to consider the patient's views on their health data being shared. A pilot program was conducted in South Korea to investigate patient opinions of HIE (Song *et al.* 2013); The researchers noted that even though patients had concerns about information safety and security, all respondents in the surveyed samples show they accepted and were willing to support HIE technology. The main reason for the positive support was the benefit of convenience when redundant procedures were removed instead of the perceived improvement in quality or cost savings.

Security and privacy: Patient health information is extremely sensitive in terms of privacy and confidentiality and it is thus, a main concern in any healthcare record systems. The integrity of medical records is also very important because the life of a patient may be dependent on the accuracy of the information. To be able to have health data when it is needed is at the very heart of HIE. To be accountable and to be able to have control are two significant aspects of authorizing and auditing access to medical records. All these criteria are basic requirements in any e-Health system and becoming more persistent when data are moved outside their original domain and shared with outside parties. Permitting users to access information from virtually anywhere and anytime radically enlarges the universe of illegal intruders which seriously complicate the form and use of a secure system (Wasserman, 2011).

Related EHR security policies/standards: The legislating of privacy policies has been done in many countries for the purpose of regulating and safeguarding the privacy of patient records. For instance, the US Health Insurance Portability and Accountability Act (HIPAA) controls the privacy and security of US patient data. These policies may vary for different countries. Moreover, EHRs themselves are regulated by standards which comprise security and privacy terms such as Health Level 7 (HL7), to ensure data security and privacy. Through the combination of these standards and security mechanisms applied by providers, a secure EHR will be achieved. Unfortunately, the policies that can be used to evaluate and enhance the security of EHR are limited. The following paragraphs briefly discuss the relevent policies/standards.

Personal Data Protection Act 2010: In Malaysia, healthcare organizations in respect of Electronic Medical Records (EMRs) have to take into consideration privacy issues in their organization in order to comply with the Personal Data Protection Act (PDPA) 2010 which was enforced on 15 November 2013. The biggest problem in Malaysia is the protection of privacy and confidentiality of stored medical data. This is due to the fact that people are not generally aware of privacy concerns as it pertains to medical data. Consequently, Malaysians are not conscious of the danger that their personal data could be at risk of violation and their privacy invaded. Furthermore, Malaysia dies not have an adequate legal framework to protect data (Bennani *et al*., 2008). However, there appears to be a shift towards greater concern among Malaysians about the privacy of their medical data. A new bill has been proposed by the Malaysian Ministry of Energy, Communications and Multimedia (MECM). The first legislation was the Personal Data Protection (PDP) Bill in 1998 then there was a second PDP Bill in 2001, a third (Personal Data Protection Bill (No. 1) 2009) and finally the Personal Data Protection Act (2010) (Bennani *et al*., 2008). After a few amendments, the bill was passed in January 2011 and is known as the PDP Act 2010 (Ferreira *et al*., 2011). The PDP Act controls the collection, possession, processing and use of personal data by any person or organization for the protection of an individual's personal information.

Health Insurance Portability and Accountability Act (HIPAA): The United States HITECH (Health Information Technology for Economic and Clinical Health) legislation, passed in February 2009 is a follow-up on the federal government's earlier HIPAA (Health Insurance Portability and Accountability Act) legislation and provides plans for required privacy and security controls on digital healthcare systems. HIPAA encompaassed privacy and security rules that came into effect in 2005. HITECH comprises additional new requirements for reporting breaches. This means that there must be data encryption and health practitioners must destroy unencrypted copies of health information after use. Medical data used for research must be confined to the information related to the study and with patient identity suitably obsecured. Furthermore, HITECH raised the HIPAA penalties for both inadvertent and willful disclosure of unsecured patient information (Liu and Park, 2011).

Information Security Management System (ISMS): The phenomena of rapid growth and rising frequency of cyber-attacks has prompted organizations to adopt security standards and guidelines. International Organization for Standardization and the International Electro technical Commission (ISO/IEC) have developed the ISO/IEC 27000 series of standards specifically matters related to information security. Through ISO/IEC 27001 Information Security Management System (ISMS)-requirements an organization may comply with and obtain the certification to increase the protection level for their information and information systems. Information security metrics can prove useless if organizations fail to have data to measure, procedures or processes as guides, indicators to facilitate good protection decisions and human resources to develop and report to the management.

Confidentiality, Integrity and Availability (CIA) triad model: The National Institute of Standards and Technology defines information security as the preservation of data's confidentiality, integrity, availability and accountability (commonly referred to as the "CIA" Triad). Confidentiality in this definition refers to "The ability to make data available to authorized persons or processes". For example, a medical record of a cardiac patient which reveals a diagnosis of HIV would be

undisclosed from cardiology researchers if HIV status is irrelevant to their research (Rodriguez *et al*., 2011). Integrity refers to "the ability to maintain data or information or the ability to prevent the data or information from being altered in an unauthorized manner." Integrity according to the National Institute of Standards and Technology is defined as guarding against improper information modification or destruction. It also guards against accidental damage to the system. Integrity ensures that changes made to the system by authorized users do not result in loss of data consistency. Hence, data integrity makes sure the data are precise and complete without any unauthorized modifications or alterations. Availability refers to the ability to ensure that data or information are accessible and useable by authorized persons in a timely manner. According to Petkovic *et al*. availability is the ability of up-to-date information to be accessible when needed at a required level of performance and at the appropriate place. Data availability are seen to be more vital than data confidentiality, especially in emergency cases. Accountability refers to "The ability to audit, review as well as appraise the actions of all parties and processes which interact with the information and to determine if the actions are appropriate."

Malaysia IHE (MyHIX): In 2007, MOH proposed the Integrated Health Enterprise (IHE) framework. This framework then proposed connection: a (Connectivity marATHON) which MSC Malaysia and the Ministry of Health (MOH) jointly organized. Vendors or healthcare service providers who had data sharing solutions took the opportunity to test how their offerings complied based on HL7 standard in a realistic and live interoperability environment (Fink, 2005). Taking into consideration the significance of creating an integration engine and the earlier challenges faced in the implementation of such engine, MOH introduced a novel initiative in 2008 funded by the Multimedia Development Corporation. The new project is the Malaysian HIE (MyHIX) which is the integration engine in the IHE framework. It provides the sharing of patient discharge summary among the facilities of the MOH.

MATERIALS AND METHODS

The purpose of this study is to analyseze the available security frameworks for EHR in order to determine their strength and limitations. The analysis later enables the identification of research areas concerning EHR security that could be explored further. Generally, the study endeavoured to answer the Research Questions (RQ).

What are the factors that contribute to the safety of electronic health records? How can these factors be combined in the form of an integrated security-related framework?

This study adopted a qualitative approach as it is deemed suitable for answering the above RQs. This approach allows researchers to understand and investigate the research topic in depth and in comprehensively. The specific qualitative technique used in the study was reviewed in the literature. Reviews involved the process of identifying and examining secondary data sources based on certain topics of interest as well as the evaluation of specific problems. The technique is beneficial as it avoids repetition. It allows the identification of factors that influence the research problem from references that are appropriate in the context of studies such as journals, books, conference proceedings and organizational reports.

The study was based on the literature review of earlier studies. Thus, Systematic Literature Review methodology (SLR) was used to suggest an assessment model of the various levels of implementing information security. SLR is a systematic, clear, detailed and reproducible technique to identify, evaluate and synthesize the existing body of completed and recorded knowledge (Fink, 2005).

The reviews in the study were conducted systematically and covered various references concerning security and EHR. The search was made by using the following keywords: "Security and EHR", "Security model", "Security" or "Safety" or "Privacy" and "Factor". Among the databases that were used in the search were IEEE Explore, Emerald, Jstor, ISI Web of Science, ProQuest, Science Direct and Springer. This study also used snowball technique in which investigation was made of the relevant publications based on the reference lists. As the results of the search were massive, exclusion criteria were set. For instance, the study excluded references on interaction design as its focus is very much concerned with system interface design. After carrying out the exclusion activities, the shortlisted references were analyzed by employing content analysis which required separating the data and examining the prevalence of category occurrences. The process was conducted continuously for the duration of the study. The purpose of the content analysis was to identify the common security themes in the selected references.

RESULTS AND DISCUSSION

In our study, we ovserved that there was no EHR security solution in the literature to be used as examples for end-to-end security control. Solutions in the current

Table 1: Summary of product solution

Variables	Summary
Record actions related to EHI (i.e., auditlog)	The date, time, patient identification (name or number) and user identification (name or number) must be recorded when EHI is created, modified, deleted or printed. An indication of which action(s) occurred must also be recorded (e.g., modification)
Cross-enterprise authentication	Use of a cross-enterprise secure transaction that has enough identity information to enable the receiver to access control decisions and produce comprehensive and precise security audit trails
Record treatment, payment and health care operations disclosures	The date, time, patient identification (name or number), user identification (name or number) and a description of the disclosure must be recorded
Authentication to control who is connecting to EHR exchange network and applications	Accounts/passwords, kerberos, security tokens/IDs, biometrics
Authorization to control who can access what EHR information	Files and DB access control, access control lists; Role/need-limited access: enabling access for personnel only to information essential to the performance of their jobs and limiting the real or perceived temptation to access information beyond a bona fide need
Privacy: the right and desire of a person to control the disclosure of personal health information	Digital signature for controlled release of personal health information to a care provider or information custodian under an agreement that limits the extent and conditions under which that information may be used or released further
EHR security the perimeters	Firewall and network service management; wireless security protocols. Knowing and controlling the boundaries of trusted access to information system, both physically and logically
Information right management	Control information distribution, ensure record owners, data stewards and patients can understand and have effective control over appropriate aspects of information security and access
Accountability	Helping to ensure that healthcare providers are responsible for their access to and use of information, based on a documented need and right to know. Audit logs are maintained regularly
Availability	Network and application monitor tools to prevent Denial-of-service attacks, ensuring that accurate and up-to-date information is available when needed at appropriate places
Confidentiality	Healthcare professionals are more concerned to gain trust from the patient by maintaining the appropriate degree of confidentiality
Integrity	Securing the integrity of medical records is important because the life of the patient may depend on the correctness of the health information

Table 2: Comparison of PDPA 2010, HIPAA, ISMS, CIA and MYHIX

Elements	Personal Data Protection Act 2010	Health Insurance Portability and Accountability Act (HIPAA)	Information Security Management System (ISMS)	Confidentiality, Integrity and Availability (CIA) Triad Model	Malaysian HIE (MYHIX)
Scope and security	Focuses on: Patient Safety data	Focuses on: Privacy Safety data Encryption	Focuses on: Security Interface specifications Standards	Focuses on: Confidentiality Integrity Availability	Focuses on: Security Interface specifications Standards
People	Stakeholders such as citizens, public and private organizations as well as developers with different roles and responsibilities	People who interact with the service, possess various knowledge and skills	Not applicable	People who interact with the service, possess various knowledge and skills	Stakeholders such as citizens, public and private organizations and also developers with different roles and responsibilities
Technology	ICT infrastructure and equipment's such internet, mobile, collaboration tools and applications	Hardware, software and other related system	Hardware, software and other related system components	ICT infrastructure and equipment's	ICT infrastructure and equipment's

market typically adopt a point-to-point secure socket transport with product level solutions as summarized (Table 1).

The reviews have found 4 policies and 1 framework that are related to security of EHR as shown in Table 2. The brief descriptions of these policies and framework have been described in earlier section. Subsequently, the gaps are identified which can lead to further research.

CONCLUSION

Without information security, EHR has little chance of long-term success. Security is an important element of product quality, particularly for EHR. This study has reviewed multiple security policies and frameworks. It is found that several important security attributes such as accountability, availability, confidentiality, integrity and safety can be considered in measuring the security of EHR. We have design a framework that combining three main factors which are environment, system development and product's quality attributes. All the factors are interrelated in contributing the product's security. The key contributions of our design and solutions are illustrated in the diagram.

REFERENCES

Anonymous, 2010. Overview of international EMR/HER markets: Results from a survey of leading health care companies. Accenture Management Consulting Company, Dublin, Ireland. https://www.slideshare.net/sjcherian/overview-of-international-emr-and-ehr-markets

Anonymous, 2012. Third annual benchmark study on patient privacy & data security. Ponemon Institute, Traverse City, MI, USA. https://www.ponemon.org/news-2/45

Benli, S., U. Clark, R. Vetter, B. Reinicke and S. Mitchell, 2012. Information security blueprint for national health information network. Ann. Master Sci. Comput. Inf Syst., 6: 1-13.

Bennani, A., M. Belalia and R. Oumlil, 2008. As a human factor, the attitude of healthcare practitioners is the primary step for the E-health: First outcome of an ongoing study in Morocco. Commun. IBIMA., 3: 28-34.

Blumenthal, D., 2011. Wiring the health system-origins and provisions of a new Federal program. N. Engl. J. Med., 365: 2323-2329.

Brailer, D.J., 2005. Interoperability: The key to the future health care system. Health Affairs, 24: W5-19-W5-21.

Ferreira, A., C.R. Cruz and L. Antunes, 2011. Usability of authentication and access control: A case study in health care. Proceedings of the 2011 IEEE International Conference on Carnahan Security Technology (ICCST), October 18-21, 2011, IEEE, Porto, Portugal, ISBN:978-1-4577-0902-9, pp: 1-7.

Fink, A., 2005. Conducting Research Literature Reviews: From the Internet to Paper. 2nd Edn., Sage Publications, Thousand Oaks, California, Pages: 245.

Garets, D. and M. Davis, 2006. Electronic medical records vs. electronic health records: Yes, there is a difference. MSc Thesis, HIMSS Analytics, Chicago, Illinois.

Kaelber, D.C. and D.W. Bates, 2007. Health information exchange and patient safety. J. Biomed. Inf., 40: S40-S45.

Kellermann, A.L. and S.S. Jones, 2013. What it will take to achieve the as-yet-unfulfilled promises of health information technology. Health Affairs, 32: 63-68.

Kuperman, G.J., 2011. Health-information exchange: Why are we doing it and what are we doing?. J. Am. Med. Inf. Assoc., 18: 678-682.

Kuperman, G.J., J.S. Blair, R.A. Franck, S. Devaraj and A.F. Low *et al.*, 2010. Developing data content specifications for the nationwide health information network trial implementations. J. Am. Med. Inf. Assoc., 17: 6-12.

Liu, W. and E.K. Park, 2011. E-health service characteristics and QoS guarantee. Proceedings of the 20th International Conference on Computer Communications and Networks, July 31-August 4, 2011, Maui, HI., pp: 1-5.

Payne, T.H., D.E. Detmer, J.C. Wyatt and I.E. Buchan, 2010. National-scale clinical information exchange in the United Kingdom: Lessons for the United States. J. Am. Med. Inf. Assoc., 18: 91-98.

Rodriguez, A.S., D.L.I. Torre and A.D. Pascual, 2011. [Analysis of aspects of interest on privacy and security in the Electronic Health Record (In Spanish)]. J. Electron. Eng., 7: 1-8.

Sekaran, U. and B. Roger, 2010. Research Methods for Business: A Skill-Building Approach. 5th Edn., John Wiley and Sons Ltd., UK.

Shapiro, J.S., J. Kannry, M. Lipton, E. Goldberg and P. Conocenti *et al.*, 2006. Approaches to patient health information exchange and their impact on emergency medicine. Ann. Emergency Med., 48: 426-432.

Smith, H.J., T. Dinev and H. Xu, 2011. Information privacy research: An interdisciplinary review. MIS. Q., 35: 989-1016.

Song, M., K. Liu, R. Abromitis and T.L. Schleyer, 2013. Reusing electronic patient data for dental clinical research: A review of current status. J. Dent., 41: 1148-1163.

Symantec, 2012. Internet security threat report. Volume 17, Symantec Corporation, Cupertino, CA., USA.

Walker, J., E. Pan, D. Johnston and J. Adler-Milstein, 2005. The value of health care information exchange and interoperability. Health Affa., 24: W5-10-W5-18.

Wasserman, R.C., 2011. Electronic Medical Records (EMRs), epidemiology and epistemology: Reflections on EMRs and future pediatric clinical research. Acad. Pediatrics, 11: 280-287.