Security Issues in Electronic Health Record

Fiza Abdul Rahim[a,*], Zuraini Ismail[a], Ganthan Narayana Samy[a]

[a]*Advanced Informatics School, Universiti Teknologi Malaysia, Jalan Semarak, 54100 Kuala Lumpur, Malaysia.*

Abstract

The availability of healthcare record in electronic format is an effort by the health care industry to improve the quality and reduce the cost of healthcare services. It is important to secure the records in healthcare environment which is referring to electronic health record (EHR). EHR is a computerized health record created by healthcare organization that delivers healthcare services such as hospital. The adoption of EHR, required increasing need for information exchange across multiple organizations, which is often outsourced to be stored at a third party such as cloud providers. This paper presents an analysis on a literature review findings concerning the security issues of EHR to highlight the need of security in healthcare field.

Keywords: Security issues; Electronic health record; Literature review; Healthcare; Hospital information system

1. Introduction

The effect of information technology (IT) in our lives can be seen all around us and the growth of information systems in recent years has been extraordinary in diverse working environments. The power of computing has risen dramatically and most of our daily jobs can be replaced with the technology. The majority of organizations nowadays encounter information systems as part of their daily routine. For instance, we can track and record financial transactions in accounting information system (AIS) [1]. In education field, we can manage student's basic information, class management and score management through student information system [2]. In any organization, we can capture, manage, distribute and work with documents by using document management system (DMS) [3]. Healthcare, as with any other field, there are number of hospital information systems (HIS) are currently assisting clinicians in providing efficient and quality care in healthcare institutions [4].

* Corresponding author. *E-mail address*: fiza2@live.utm.my

Most organizations continue to invest technology to provide automation in the healthcare services. In large organizations, HIS are synonym with maintaining electronic health records (EHR), clinical decision support systems and various HIS to provide efficient service, reduce costs, improve quality care and outcomes [5]. For smaller organizations, most of HIS focused are primarily in clinic management system especially in private clinics [4]. And there is a need also to share the data among health care practitioners and other related healthcare institutions such as hospital, nursing home, physicians and etc. [6].

In this paper, we review the background of EHR, covering various definition of EHR and the importance of ensuring EHR secured in HIS. Several security issues of EHR will be discussed in this paper from many different perspectives, while each focusing on dimensions of security.

1. Background

Being connected to the Internet, with such a lot of facilities, users can share and exchange information with others. This can be seen with enormous developments in mobile devices and web-based applications in healthcare field in the past few years [7-9]. While the Internet also providing such a lot of facilities and allowing users to share and exchange information, which may include sensitive information of the patients using paper-based, personal-computer based, memory devices, portal and networked EHR [5].

Electronic record allowed users to increase the accessibility of sharing the records among individuals or groups. In medical informatics research, the idea of EHR has been around for more than 20 years. EHR contains of healthcare information about an individual's lifetime with the purpose of supporting continuity of care, education and research and ensuring confidentiality at all times [10].

EHR also referred as a "personal information containing identification, demographic information, history of medical diagnosis, digital renderings of medical images, treatments, medication history, dietary habits, allergies, sexual preference, genetic information, psychological profiles, employment history, income and physicians' subjective assessments of personality and mental state" [10-13]. The London School of Economics and Political Science reported that HIS "cover a wide range of information and communication technologies, from EHR to systems for managing and tracking patients, test results, medications, disease and so forth" [14]. As a general, EHR can be considered as healthcare resources of patient having their healthcare services and cares in a specific or several healthcare institutions that can be retrieved electronically.

Over the past two decades, most scholars stated that if the record is related in health information, ensuring the privacy of information collected during healthcare processes is necessary [5, 6, 14-21]. When the privacy becomes the main important issues in handling EHR, there is a need to ensure the security throughout the entire healthcare processes.

In U.S, all academic medical centers (AMSs) and other related entities must comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 but several studies shown most of the AMSs and other related institutions are not fully complying with HIPAA security [22]. In Title II of HIPAA, it is clearly mentioned about the procedure to assure that any information is utilized and protected appropriately to ensure the confidentiality of the information and the privacy of individuals receiving healthcare services and items [23].

For a patient to get diagnose and treatment from healthcare professionals, he or she is required to share information to avoid adverse drug interactions [5]. However, the patient may refuse to give information about health problems such as HIV. As stated in UNAIDS Political Declaration on HIV [24], public health goals must use EHR in balance against individual's rights to privacy and confidentiality and such information related with HIV status must be kept confidential.

From all those literatures about EHR, two main keywords are always comes together: privacy and confidentiality. These two keywords are among of the key concepts of information security [25]. Privacy means that information will be used only in ways known to the person providing it while confidentiality of information ensures that only those with sufficient privileges may access certain information.

Based on the distinction between the terms of privacy, confidentiality and information security, EHR must comply all those three terms: (1) EHR must be handled by ensuring the privacy of an individual to control disclosure of EHR [5, 16, 18]; (2) EHR must only be disclosed to any authorized users at specific times of need to ensure the confidentiality [5, 16, 19]; and (3) EHR must be secured throughout the healthcare processes to protect from unauthorized destruction, modification and disclosure [5, 16, 19].

2. Method

This literature review was performed with searches in IEEExplore and ScienceDirect database. Due to the highly number of results obtained, we filtered the abstracts following several criteria: (1) English as language; (2) Articles with less than 5 years;

and (3) A cautiously reviews of the abstracts to exclude articles with the same or outdated information.

The search strategy is explained in more details in the following:

- Searching the combination of phrases "security issues" and "electronic health record" returned 50 articles where 38 of them were selected for further studies.
- On these 38 studies, only 20 turned out to be relevant to the review.

3. Result and Discussion

In this section, we present a review of the information security literature in healthcare field.

a. Privacy Concerns and Threats

A study conducted to explored patients' views about sharing of EHR [19]. The result showed that the patients are clearly agreed about electronic health information exchange (HIE) in order to improve the quality of healthcare services but they also worried about the potential of security breach and misuse of their health data by unauthorized party. A report produced by The London School of Economics and Political Science [14] also stated that the greatest threats to an organization's information assets come from within.

However, the organization also must consider the threat from external of medical information. HIS may be exposed with the risk of external abuse of EHR, but the problem cannot be solved in technological ways only, it must come along with organizational nature as well such as how they can ensure their patients' information in recorded securely and will guard patient privacy [26].

Based on the fundamental security goals [27], there are three important goals that must be comply: (1) confidentiality; (2) integrity; (3) availability (CIA). For EHR, it is critical to protect and secure the information to ensure the CIA of EHR [28]. In ISO EN13606 standard [29], confidentiality refers to the "process that ensures that information is accessible only to those authorised to have access to it", integrity refers to the "duty to ensure that information is accurate and is not modified in an unauthorised fashion" and availability refers to the "property of being accessible and usable upon demand by an authorised entity". The confidentiality of EHR is essential if the privacy of the patient is to be maintained, the integrity of EHR is must to ensure patient safety and ensuring the information's entire life cycle is fully auditable and the availability of EHR is also critical to effective healthcare delivery [28].

b. Access Control

Managing access control is one of the main important security issues in HIS because EHR resides in a large networked system and a number of users may accessing EHR for several purposes within and across their department. For example, pharmacist may need to access to a specific patient data to identify which medicine that has been prescribed by the patient's physicians to avoid mistake by giving a wrong drug.

There are two kinds of authentication have been distinguished: user authentication and data authentication [28]. Most of the findings of this review have shown that Role-Based Access Control (RBAC) model has been used to access EHR [15, 30, 31]. Access to EHR should be on a "need to know" basis [16]. RBAC can be applied to manage access control by granting an access based on the role of each person in the provision of patient care [5, 16, 32]. RBAC can be an effective tool to manage such a complex role hierarchies in healthcare organizations [33]. Similar to privacy concerns and threats domain, access control cannot be solved in technical solution only. It requires consideration of healthcare organizations to clearly identify work processes, organizational structure and culture to provide effective information security [34].

c. Health Information Exchange (HIE)

Most of EHR provides sharing within the same organization easily but sharing across organizations is completely disaster [6]. Healthcare professionals may share their patients' information with another party who are not part of the same organizational entity. And healthcare organizations may have their own developer to design their intended HIS and the information stored in the system can be in different formats without standardization with another healthcare providers, insurance company and so forth.

In U.S, there are several efforts to solve the complicated issues of HIE have been made by regional health information organizations (RHIO) [35], Health Information Technology for Economic Clinical Health (HITECH) Act [36] and the latest one is the Direct Project [37]. But there are several barriers to solve HIE issues [6]: (1) data privacy and security; (2) non-structured data; (3) meaningful use of HIE because of infrequently participate in HIE; (4) competitive implications of sharing data between healthcare providers; and (5) convincing health care professionals the demand of EHR and use them when available is useful for reviewing patient data from past.

It would be much more easier if the decision has been made to solve this issue because if there is standardization or common disclosure information is constructed for EHR, it may help to speed up the transfer process between different healthcare providers and

also can ensure only "need to know" information or specific protected disclose information are being transferred to another authorized party.

d. Information Security Policy

Healthcare institutions must manage information security risks in a proper way by adopting information security policy to minimize financial losses from potential security incidents. A few years ago, there have been few activities in policy development involving privacy issues of EHR [38]. Policy is the essential foundation of an effective information security program [25]. Therefore, there is a need for business continuity planning in case of any internal or external threats may disrupt operations in the organization [5]. One policy in a healthcare institutions may not working in other healthcare providers because policy must be customized based on organizational culture, employee behavior, customer expectations, potential security incidents and etc.

e. Cloud Computing

The latest technological trends, Cloud Computing (CC) provide a strong infrastructure for HIS services over the Internet [21]. CC can be defined as "A computing paradigm which is a pool of abstracted, virtualized, dynamically scalable, managing, computing, power storage platforms and services for on demand delivery over the Internet" [39]. CC has opened an opportunity for healthcare organization to share part of the data with others, such as government agencies, other healthcare providers, insurance companies and etc. by centralizing their EHR on the Cloud [21, 39, 40].

However, centralization of EHR on the Cloud may result in a number of risk such as data security risks, the risk of loss of data and the risk of systems unavailability [21]. Security and privacy protection of EHR in the Cloud is importance as protection of EHR which are not in the Cloud because it is still containing patients' information that must be protected all the time.

The discussion of five security issues in EHR is summarized in Table 1.

Table 1. Security Issues in Electronic Health Record

Security Issues	Details
Privacy Concerns and Threats	Ensure the privacy of EHR from internal and external threats.
Access Control	Identify work processes, organizational structure and culture of the healthcare organization to manage access control.
Health Information Exchange	Ensure the "need to know" information to speed up the transfer process.
Information Security Policy	Customize the policy based on organizational structure, employee behavior, customer expectations, potential security incidents and etc.
Cloud Computing	Identify protection mechanism to protect EHR in the cloud.

4. Limitation

There are number of limitations in this review. The studies review used keywords to retrieve the existing literatures; therefore those studies without the main keywords that have been used for this review may not be included. Second, the review focused on EHR definitions in selected literature only. However, the studies reviewed several security issues in different perspective to be integrated with future security research of EHR.

5. Conclusion

A literature review of security issues in EHR was presented in this paper with emphasis on the importance of protecting privacy and confidentiality of EHR. We highlighted five different security issues of EHRs based on the current trends of HIS. From the literature, most of the security issues in EHR are focusing on the privacy and confidentiality of patients' information. It is a must for healthcare providers to protect EHR embedded in their HIS for a proper retrieval by authorized users.

To get better understanding of security issues of EHR, it is important to identify the current problems at different views of users. By identifying the security problems or risks that may occur, there is a need of appropriate approaches to encounter the problems. This is necessary because there is no doubt that the security in EHR is important to ensure the privacy and confidentiality of EHR throughout the healthcare services and care.

Acknowledgement

This work is funded by Zamalah Scholarship provided by Universiti Teknologi Malaysia (UTM) and Research University Grant from UTM and Ministry of Higher Education (MOHE) Malaysia with the project number Q.K 130000.2138.01H98.

References

[1] V. S. Maziyar Ghasemi, Mohammad Aslani, Elham Barvayeh, "The impact of Information Technology (IT) on modern accounting systems," in *Procedia - Social and Behavioral Sciences*, 2011, pp. 112-116.

[2] Z. W. Liu, Huixia ; Zan, Hui "Design and Implementation of Student Information Management System," in *2010 International Symposium on Intelligence Information Processing and Trusted Computing (IPTC)* ed: IEEE, 2010, pp. 607- 610.

[3] M. Jiajia, F. Zhongjun, C. Guoyou, M. Handong, and W. Le, "A Private Cloud Document Management System with Document Clustering Algorithm," presented at the National Conference on Information Technology and Computer Science (CITCS 2012), lanzhou, China, 2012.

[4] P.-Y. Yen and S. Bakken, "Review of health information technology usability study methodologies," *J Am Med Inform Assoc*, pp. 1-10, 2011.

[5] A. Appari and M. Eric Johnson, "Information security and privacy in healthcare: current state of research," *Int. J. Internet and Enterprise Management*, vol. 6, pp. 279-314, 2010.

[6] J. Adler-Milstein and K. J. Ashish, "Sharing Clinical Data Electronically: Critical Challenge for Fixing the Health Care System," *Journal of the American Medical Association*, vol. 307, pp. 1695-1696, 2012.

[7] J. M. Haakon Bryhni and C. M. Ruland, "Secure Solution for Mobile Access to Patient's Health Care Record," presented at the IEEE 13th International Conference on e-Health Networking, Applications and Services, Columbia, USA, 2011.

[8] F. Mancini, S. Gejibo, K. A. Mughal, R. A. B. Valvik, and J. Klungsøyr, "Secure Mobile Data Collection Systems for Low-Budget Settings," presented at the 2012 Seventh International Conference on Availability, Reliability and Security, Prague, Czech Republic 2012.

[9] I. Ćubić, I. Markota, and I. Benc, "Application of Session Initiation Protocol in Mobile Health Systems," presented at the 33rd International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, Croatia, 2010.

[10] I. Iakovidis, "Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe," *International Journal of Medical Informatics*, vol. 52, pp. 105-15, 1998.

[11] R. T. Mercuri, "The HIPAA-potamus in health care data security," *Communications of the ACM*, vol. 47, pp. 25–28, 2004.

[12] D. Urda, N. Ribelles, J. L. Subirats, L. Franco, E. Alba, and J. M. Jerez, "Addressing critical issues in the development of an Oncology Information System," *International Journal of Medical Informatics*, 2012.

[13] B. Blobel, "Advanced and secure architectural EHR approaches," *International Journal of Medical Informatics*, vol. 75, pp. 185-90, 2006.

[14] "Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations " The London School of Economics and Political Science, 2010.

[15] C. Randolph, J. Barrows, and P. D. Clayton., "Privacy, Confidentiality and Electronic Medical Records," *Journal of the American Medical Informatics Association*, vol. 3, pp. 139-148, 1996.

[16] G. Kurtz, "EMR Confidentiality and Information Security," *Journal of Healthcare Information Management*, vol. 7, pp. 41-48, 2002.

[17] L. M. Lee and L. O. Gostin, "Ethical Collection, Storage, and Use of Public Health Data: A Proposal for a National Privacy Protection," *Journal of the American Medical Association*, vol. 302, pp. 82-84, 2009.

[18] M. A. Hall and K. A. Schulman, "Ownership of Medical Information," *Journal of the American Medical Association*, vol. 301, pp. 1282-1284, 2009.

[19] S. R. Simon, J. S. Evans, A. Benjamin, D. Delano, and D. W. Bates, "Patients' Attitudes Toward Electronic Health Information Exchange: Qualitative Study," *Journal of Medical Internet Research*, vol. 11, p. e30, 2009.

[20] I. Carrión Señor, J. Fernández-Alemán, and A. Toval, "Are personal health records safe? A review of free web-accessible personal health record privacy policies," *Journal of Medical Internet Research*, vol. 14, p. e114, 2012.

[21] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, "e-Health Cloud: Opportunities and Challenges," *Future Internet*, vol. 4, pp. 621-645, 2012.

[22] J. W. Brady, "Securing Health Care: Assessing Factors that Affect HIPAA Security Compliance in Academic Medical Centers," in *Proceedings of the 44th Hawaii International Conference on System Sciences*, Hawaii, 2011.

[23] "Health Insurance Portability and Accountability Act of 1996," U. S. Government, Ed., ed. U.S: U.S Government Printing Office, 1996, pp. 104-736.

[24] "UNAIDS Political Declaration on HIV," UNAIDS, 2006.

[25] M. E. Whitman and H. J. Mattord, *Management of Information Security*, Second ed. Canada: Thomson Course Technology, 2008.

[26] T. C. Rindfleisch, "Privacy, Information Technology, and Health Care," *CACM*, vol. 40, pp. 92-100, 1997.

[27] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, and N. Muller, "Aspects of privacy for electronic health records," *International Journal of Medical Informatics*, vol. 80, pp. 26-31, 2011.

[28] I. C. S. José Luis Fernández-Alemán, Pedro Ángel Oliver Lozoya, Ambrosio Toval, "Security and privacy in electronic health records: A systematic literature review," *Journal of Biomedical Informatics*, pp. 1-22, 2013.

[29] ISO, "ISO/EN 13606," ed.

[30] A. Boxwala, J. Kim, J. Grillo, and L. Ohno-Machado, "Using statistical and machine learning to help institution detect suspicious access to electronic health records," *Journal of the American Medical Association*, vol. 18, pp. 498-505, 2011.

[31] A. Ferreira, -. C. Cruz, R., L. Antunes, and D. W. Chadwik, "Access control: how can it improve patients' healthcare?," *International Journal of Medical Informatics*, vol. 127, pp. 65-76, 2007.

[32] V. C. Hu, D. F. Ferraiolo, and D. R. Kuhn, "Assessment of Access Control Systems," National Institute of Standards and Technology (NIST), 2006.

[33] M. P. Gallaher, A. C. O'Connor, and B. Kropp, "The Economic Impact of Role-Based Access Control," National Institute of Standards and Technology (NIST), 2002.

[34] A. Ferreira, -. C. Cruz, R., L. Antunes, P. Farinha, E. Oliveira-Palhares, D. W. Chadwik, *et al.*, "How to break access control in a controlled manner," in *IEEE Symposium on Computer-Based Medical Systems*, Maribor, Slovenia, 2006, pp. 847-854.

[35] W. Raghupathi and S. Kesh, "Interoperable electronic health records design: towards a service-oriented architecture," *e-Service Journal*, vol. 5, pp. 39-57, 2007.

[36] "Meaningful Use Workgroup Request for Comments Regarding Meaningful Use Stage 2," Health Information Technology Policy Committee, 2012.

[37] G. Kuperman, "Health-information exchange: why are we doing it, and what are we doing?," *J Am Med Inform Assoc.*, vol. 18, pp. 678-682, 2011.

[38] M. Rothstein, "Health privacy in the electronic age," *J Leg Med*, vol. 28, pp. 487-501, 2007.

[39] I. Foster, Y. Zhao, L. Raicu, and S. Lu, "Cloud Computing and Grid Computing 360-Degree Compared," in *Proceedings of the Grid Computing Environments Workshop (GCE)*, Austin, TX, USA, 2008, pp. 1-10.

[40] C. Chatman, "How cloud computing is changing the face of health care information technology.," *Journal of Health Care Compliance*, 2010.