Privacy Challenges in Electronic Medical Records: A Systematic Review

Fiza Abdul Rahim, Zuraini Ismail and Ganthan Narayana Samy
Advanced Informatics School (AIS)
Universiti Teknologi Malaysia (UTM)
54100 Kuala Lumpur, Malaysia
fiza2@live.utm.my, zurainiismail.kl@utm.my, ganthan@ic.utm.my

ABSTRACT

Various types of data, including demographics and clinical information, are continuously collected and stored in the form of electronic medical records (EMR). Such data have been traditionally used to facilitate the workflow of healthcare, but now it is recognized as an important source for healthcare analysis and decision making. In Malaysia, with regards to EMR, healthcare providers need to ensure that their organization comply with Personal Data Protection Act (PDPA) 2010. As EMR are continued to be disseminated to other parties aside from healthcare providers, it may pose serious threats to patients' privacy. Thus, it is important for healthcare providers to understand the privacy challenges in EMR before implementing adequate mechanisms to protect EMR privacy. This paper presents systematic literature review (SLR) results to categorize privacy challenges in EMR.Selected Malaysian healthcare providers are chosen to participate in this study. Ultimately, the findings of the study may assist healthcare providers in designing and implementing privacy mechanisms of EMR towards the compliance of PDPA 2010.

Keywords: privacy, sharing, electronic medical records.

I INTRODUCTION

A report from Ponemon Institute (2012) discovered that most healthcare providers struggle to deal with privacy risks due to lack of technologies. Another report from Symantec (2013) found that healthcare recorded the highest percentage of disclosed data breaches based on industry. With the exposure of various types of potential privacy breaches with electronic medical records (EMR) (Samy, Ahmad, & Ismail, 2009), healthcare providers must manage privacy risks in a proper way by adopting an adequate security mechanism (Abdul Rahim, Ismail, & Samy, 2013b, 2014; Bakhtiyari Shahri & Ismail, 2012; Hassan & Ismail, 2012; Samsuri, Ismail, & Ahmad, 2011). Before implementing any security mechanism, it is important for the healthcare providers to identify the current problems or challenges in the EMR system.

A number of systematic reviews have already been conducted in the privacy domain. However, none of them involved direct observation of the privacy challenges faced by the healthcare providers. Hence, this systematic review is to fill this gap that is to review, identify, and categorize privacy challenges in EMR. The following section highlights on the need of privacy in EMR. Next, the third section describes the review method used in this study. The fourth section reports the findings and discussions. To end, the final section concludes the entire paper.

II EMR SHARING AND THE NEED FOR PRIVACY

EMR need to be shared among healthcare practitioners or healthcare providers to improve healthcare provisioning and medical research (Abdul Rahim, Ismail, & Samy, 2013a). In another perspective, EMR need to be shared to allow data utility to support medical research, decision making, personalized medicine and etc. (Li & Qin, 2013). Therefore, it is crucial to ensure the privacy of EMR because it is not just a record but contain patients' sensitive information.

III REVIEW METHOD

This review process uses the systematic literature review (SLR) guidelines for information system research by Okoli & Schabram (2010) and Petticrew & Roberts (2006). There are four main stages: planning, selection, extraction and execution (Okoli & Schabram, 2010). During the planning stage, the purpose and research question of this review are defined. Then, the second stage involved literature search and selecting which articles to be considered for the review. A quality assessment for each article is conducted in the third stage (Hu & Shuo, 2010). The final stage is execution which involves discussion of findings and reporting the review.

A. Research Questions

To align with the purpose of this study, the research question for this SLR is:

"What privacy challenges exist in EMR?"

B. Primary Search

The primary search process involved 5 online databases as data sources which are IEEEXplore Digital Library, ScienceDirect, ProQuest, Medline, and Taylor & Francis. The selection of databases were based on the availability of full text articles subscribed by the Universiti Teknologi Malaysia's library. The inclusion criteria involve articles published in English, available in full text, published between January 2009 and March 2014, and deal with the privacy challenges in EMR.

C. Search Strategy

The initial search strings are privacy challenges, electronic medical records, and electronic healthcare records. The search string is then constructed using Boolean "and" and Boolean "or" operators to allow synonyms and word class variants of each keyword. The resulting search string is ("privacy challenge") AND ("electronic medical record" OR "electronic health record" OR "electronic healthcare record" OR "electronic health care record").

D. Study Selection

The study selection was organized in three phases:

i. Primary Search: The search for publications from five online databases. This phase was conducted by using the search string.
ii. Exploration of title, abstract and keywords of identified articles and selection based on eligibility criteria.
iii. The selection only considered full-text articles subscribed by the Universiti Teknologi Malaysia's library.

E. Data Collection

To facilitate the data collection process, a quality checklist was used in order to gather evidence related to the research question. In designing the study's quality checklist, some of the questions listed in the previous literature were reused (Abdul Rahim et al., 2013a; Fink, 2005; Greenhalgh, 2000; Leedy & Ormrod, 2005; Petticrew & Roberts, 2006; Spencer, Ritchie, Lewis, & Dillon, 2003). There are5 general questions in the quality checklist to measure the quality of selected studies as shown in Table 1.

Table 1:Quality Checklist

No.	Item	Answer
SQ1	Are the aims and objectives of the research clearly stated?	Yes/No
SQ2	Is the research design clearly specified and appropriate for the aims and objectives of the research?	Yes/No /Partially
SQ3	Do the researcher(s) provide(s) a clear account of the process by which their findings were produced?	Yes/No /Partially
SQ4	Do the researcher(s) display(s) enough data to support their interpretations and conclusions?	Yes/No /Partially
SQ5	Is the method of analysis appropriate and adequately explicated?	Yes/No /Partially

IV FINDINGS AND DISCUSSION

The initial searching phase provided a total of 249 studies using the search string. The resulting studies' titles, abstracts and keywords were screened and only 35 were selected. Finally, after a thorough consideration, a total of 20 articles were included in the review.

From the reviews, 5 privacy issues appeared as the main privacy challenges in EMR as tabulated in Table 2, and privacy preservation and technology are found to be the most frequently discussed topic in these literatures.

Table 2: Investigated Privacy Challenges in Studies

Privacy Challenges	Study ID
Privacy Preservation	S3, S6, S7, S10, S12, S14, S18
Information Exchange	S4, S7
Technology	S1, S2, S5, S8, S14, S15, S17, S18, S19, S20
Information Storage	S9, S11, S15
Policy	S13, S14, S15, S16

1. PrivacyPreservation

Article S3, S10 and S12 agreed that the preservation of EMR privacy is the main challenge in healthcare information system (HIS). Hence, it is important for healthcare providers to offer privacy guarantee at all levels within the system (S7). As a solution, an advanced technological approach should be applied in order to retrieve and exchange EMR in a secure and reliable manner throughout the organization.

The control and access to HIS should be defined clearly to ensure that patients' privacy is not exposed to unauthorized parties (S6). Healthcare providers should establish rules to control authorization on EMR resources. In addition, selecting the best features for authentication might be the prime challenge to preserve privacy (S3, S14 and S18). Healthcare providers may implement several types of authentication technologies such as multiple biometrics for identifying users before they are allowed access to the EMR system.

2. Information Exchange

The information contained in EMR are personal and sensitive. Thus, it would involve privacy breach when the EMR is being accessed by third parties such as insurance companies or other healthcare providers (S7). These third parties may then use this sensitive information to make for profit or even for malicious motives. One example is the exploitation of EMR for marketing and advertising purposes.

In Europe, the Biobanking and Biomolecular Resources Research Infrastructure aims to facilitate collaboration between biobanks. Clients of biobanks are typically people who donates blood, tissue, and body fluid which has direct linkage of an individual's personal information including EMR. Article S4 reported that the biggest challenge for this collaboration is obtaining broad consent from different regions. It is suggested that healthcare providers give careful considerationand implement proper mechanism to protect EMR privacy of their patients.

3. Technology

In the use of location-based technologies embedded in the EMR, article S1, S2 and S19 stated that those technologies pose new challenge to privacy, as they enable third parties to locate and track people and objects anywhere and at any time. Another such technology is biometric such as heart pacemakers and internal human body medical defibrillators, where the information captured by those devices are being recorded in the EMR for further diagnosis (S5). Article S17 and S18 also highlighted the use of Radio-Frequency Identification (RFID) tags to store EMR is being identified as a privacy challenge.

Article S14 claimed that the concept of the Internet of Things (IoT) has also evolved in the healthcare domain. The data overflow caused by billions of entities creating information is a big threat to privacy. Hence, healthcare providers must possess the required tools that allow anonymity from this new technology.

With the emergence and development of mobile healthcare, several healthcare providers shift their EMR storage into cloud computing platforms (S20). Article S8 and S15 reported that by fully depending on cloud service provider, applications running on or being developed in cloud computing platforms may pose various privacy challenges such as restriction on access control mechanism and different jurisdiction of privacy regulation. Therefore, healthcare providers must provide comprehensive privacy protection in preparing themselves with the developing technologies in healthcare.

4. Information Storage

As more healthcare providers maintained EMR and shared the data between them and other institutions, another challenge associated with the EMR is information storage and access. The most common violations of EMR stored in servers are staff abuse and misuse of the right to access the records (S9). Protection of EMR can be strengthened by educating employees with the appropriate use of privileged information.

Healthcare, similar with many other industries, is creating large amounts of data to be stored, processed and analyzed (S11). In a situation which healthcare providers use cloud computing platform, the jurisdiction of regulations may become a challenge to protect EMR privacy. Article S15 reported that each cloud service provider has its own access control mechanism and users do not have an input into negotiating the terms of the contract on the mechanism to secure their data stored in these platforms. Thus, an international approach is needed between governments which could universally regulate this matter.

5. Policy

Article S14 and S15 highlighted that it is not possible to implement centralized policy if the data servers are located in foreign countries or operated by different providers. In situations where EMR is being used for consulting patients over the Internet

(S16), it also becomes another challenge to protect the privacy of EMR because it may involve different policies and jurisdictions. As discussed earlier, agreements between related governments are needed to regulate this matter.

Article S13 reported that patient privacy rules may become a challenge for healthcare providers because patients may have their own preferences with regard of their EMR. Patient privacy rules may overwrite the policies that have been defined by healthcare providers. It is the responsibility of the healthcare providers for managing and adhering to patient privacy rules.

V CONCLUSION

In today's environment, most organizations are affected by privacy and data protection requirements. However, for healthcare providers, they must address their attention to the personal information that they possessed in EMR. Given the risks and related requirements, ensuring the privacy of EMR could be the biggest challenge for healthcare providers.

In this paper, 5 main privacy challenges have been successfully categorized from a total of 20 primary articles used in the review process. Privacy preservation and technology were found to be the two most frequent issues that have been discussed in this branch of study. In preserving the EMR privacy, healthcare providers must apply appropriate methods to ensure the security and reliability of EMR transmission throughout the organization. In addition, the increase use of mobile technologies may further induce the risks of privacy violations. Consequently, it is suggested that healthcare providers ensure that selections of technologies are equipped with comprehensive privacy protection mechanisms.

The studies compiled also revealed other privacy challenges, namely information exchange, information storage, and policy. As healthcare is a regulated industry in which the privacy of EMR is paramount, it is important for healthcare providers to ensure greater protection of EMR. If healthcare providers are focused in safeguarding and improving their privacy protection mechanisms, improved patient care and trust will contribute to the success of a better healthcare system.

This in-progress study will proceed in evaluating the highlighted privacy challenges and recommending possible solutions. The unit of analysis for this study will be from selected healthcare providers in Malaysia. This study may assist healthcare providers to design or implement privacy protection mechanisms of EMR towards complying with the PDPA 2010.

ACKNOWLEDGMENT

This study is funded by Zamalah Scholarship from Universiti Teknologi Malaysia (UTM).

Articles Reviewed in this Study

Study ID	Article Details
S1	Cheung, A. S. Y. (2014). Location privacy: The challenges of mobile service devices. *Computer Law & Security Review*, *30*(1), 41–54. doi:10.1016/j.clsr.2013.11.005
S2	Damiani, M. L., & Cuijpers, C. (2013). Privacy Challenges in Third-Party Location Services. In *2013 IEEE 14th International Conference on Mobile Data Management* (pp. 63–66). Milan: IEEE. doi:10.1109/MDM.2013.67
S3	Fong, S., & Zhuang, Y. (2012). Using medical history embedded in biometrics medical card for user identity authentication: privacy preserving authentication model by features matching. *Journal of Bomedicine & Biotechnology*, *2012*. doi:10.1155/2012/403987
S4	Gaskell, G., Gottweis, H., Starkbaum, J., Gerber, M. M., Broerse, J., Gottweis, U., … Soulier, A. (2013). Publics and biobanks: Pan-European diversity and the challenge of responsible innovation. *European Journal of Human Genetics : EJHG*, *21*(1), 14–20. doi:10.1038/ejhg.2012.104
S5	Gold, S. (2013). Healthcare biometrics: solving the staff and patient security governance challenge. *Biometric Technology Today*, *2013*(8), 5–9. doi:10.1016/S0969-4765(13)70143-7
S6	Guo, R., Wen, Q., Jin, Z., & Zhang, H. (2013). An efficient and secure certificateless authentication protocol for healthcare system on wireless medical sensor networks. *TheScientificWorldJournal*, *2013*, 761240. doi:10.1155/2013/761240
S7	Hasan, O., Habegger, B., Brunie, L., Bennani, N., & Damiani, E. (2013). A Discussion of Privacy Challenges in User Profiling with Big Data Techniques: The EEXCESS Use Case. In *2013 IEEE International Congress on Big Data* (pp. 25–30). Santa Clara, CA: IEEE. doi:10.1109/BigData.Congress.2013.13
S8	Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. doi:10.1016/j.jcss.2014.02.005
S9	Kerr, P. (2009). Protecting patient information in an electronic age: a sacred trust. *Urologic Nursing*, *29*(5), 315–8; quiz 319. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/19863038
S10	Kumar, S., Nilsen, W. J., Abernethy, A., Atienza, A., Patrick, K., Pavel, M., … Swendeman, D. (2013). Mobile health technology evaluation: the mHealth evidence workshop. *American Journal of Preventive Medicine*, *45*(2), 228–36. doi:10.1016/j.amepre.2013.03.017

S11	Liyanage, H., Liaw, S.-T., & Lusignan, S. de. (2012). Accelerating the development of an information ecosystem in health care , by stimulating the growth of safe intermediate processing of health information (IPHI). *Informatics in Primary Care*, *20*, 81–87.
S12	Nageba, E., Defude, B., & Morvan, F. (2011). Data Privacy Preservation in Telemedicine : The PAIRSE Project. *European Federation for Medical Informatics*, 661–666. doi:10.3233/978-1-60750-806-9-661
S13	Petronio, S., & Sargent, J. (2011). Disclosure predicaments arising during the course of patient care: nurses' privacy management. *Health Communication*, *26*(3), 255–66. doi:10.1080/10410236.2010.549812
S14	Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279. doi:10.1016/j.comnet.2012.12.018
S15	Saxby, S. (2014). The 2013 CLSR-LSPI seminar on electronic identity: The global challenge – Presented at the 8th International Conference on Legal, Security and Privacy issues in IT Law (LSPI) November 11–15, 2013, Tilleke & Gibbins International Ltd., Bangkok, Thailand. *Computer Law & Security Review*, *30*(2), 112–125. doi:10.1016/j.clsr.2014.01.007
S16	Sharma, L. K., & Rajput, M. (2009). Telemedicine: socio-ethical considerations in the Indian milieu. *The Medico-Legal Journal*, *77*(Pt 2), 61–5. Retrieved from http://www.ncbi.nlm.nih.gov/pubmed/19731480
S17	Weber, R. H. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23–30. doi:10.1016/j.clsr.2009.11.008
S18	Wu, Z.-Y., Chen, L., & Wu, J.-C. (2013). A Reliable RFID Mutual Authentication Scheme for Healthcare Environments. *Journal of Medical Systems*, *37*(2), 9917. doi:10.1007/s10916-012-9917-0
S19	Xu, H., Teo, H., Tan, B. C. Y., & Agarwal, R. (2012). Privacy Concerns : A Study of Location-Based Services Effects of Individual Self-Protection , Industry Self-Regulation , and Government Regulation on Privacy Concerns : A Study of Location-Based Services. *Information Systems Research*, *23*(4), 1342–1363.
S20	Zhou, J., Cao, Z., Dong, X., Lin, X., & Vasilakos, A. V. (2013). Securing M-Healthcare Social Networks: Challenges, Countermeasures and Future Directions. *IEEE Wireless Communication*, *20*(4), 12–21. doi:10.1109/MWC.2013.6590046

REFERENCES

Abdul Rahim, F., Ismail, Z., & Samy, G. N. (2013a). Information Privacy Concerns in Electronic Healthcare Records : A Systematic Literature Review. In *3rd International Conference on Research and Innovation in Information Systems – 2013 (ICRIIS'13)* (Vol. 2013, pp. 504 – 509). doi:10.1109/ICRIIS.2013.6716760

Abdul Rahim, F., Ismail, Z., & Samy, G. N. (2013b). Security Issues in Electronic Health Record. *Open International Journal of Informatics (OIJI)*, *1*, 59–68.

Abdul Rahim, F., Ismail, Z., & Samy, G. N. (2014). A Conceptual Model for Privacy Preferences in Healthcare Environment. In L. Uden, L. S. L. Wang, J. M. C. Rodríguez, H.-C. Yang, & I-Hsien Ting (Eds.), *The 8th International Conference on Knowledge Management in Organizations: Social and Big Data Computing for Knowledge Management* (pp. 221–228). Springer Netherlands. doi:10.1007/978-94-007-7287-8_18

Bakhtiyari Shahri, A., & Ismail, Z. (2012). A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS. *Journal of Information Security*, *03*(02), 169–176. doi:10.4236/jis.2012.32020

Fink, A. (2005). *Conducting Research Literature Review: From Paper to the Internet*. SAGE Publications, Inc.

Greenhalgh, T. (2000). *How to Read a Paper: The Basics of Evidence-Based Medicine*. BMJ Books.

Hassan, N. H., & Ismail, Z. (2012). A Conceptual Model for Investigating Factors Influencing Information Security Culture in Healthcare Environment. In *Procedia - Social and Behavioral Sciences* (Vol. 65, pp. 1007–1012). Jakarta: Elsevier Ltd. doi:10.1016/j.sbspro.2012.11.234

Hu, Q., & Shuo, M. (2010). Does Privacy Still Matter in the Era of Web 2 . 0 ? A Qualitative Study of User Behavior towards Online Social Networking Activities. In *Pacific Asia Conference on Information Systems (PACIS)*. Retrieved from http://aisel.aisnet.org/pacis2010/2

Leedy, P. D., & Ormrod, J. E. (2005). *Practical Research Planning and Design* (Eighth edi.). Prentice Hall.

Li, X.-B., & Qin, J. (2013). A Framework for Privacy-Preserving Medical Document Sharing. In *Thirty Four International Conference on Information Systems* (pp. 1–17). Milan.

Okoli, C., & Schabram, K. (2010). *A Guide to Conducting a Systematic Literature Review of Information Systems Research* (No. 10) (Vol. 10). Retrieved from http://sprouts.aisnet.org/10-26

Petticrew, M., & Roberts, H. (2006). *Systematic Review in the Social Sciences: A Practical Guide*. Blackwell Publishing.

Ponemon Institute. (2012). *Third Annual Benchmark Study on Patient Privacy & Data Security*.

Samsuri, S., Ismail, Z., & Ahmad, R. (2011). User-Centered Evaluation of Privacy Models for Protecting Personal Medical Information. In A. A. Manaf, A. Zeki, M. Zamani, S. Chuprat, & E. El-Qawasmeh (Eds.), *International Conference, ICIEIS 2011, Kuala Lumpur, Malaysia* (pp. 301–309). Kuala Lumpur: Springer Berlin Heidelberg. doi:10.1007/978-3-642-25327-0_26

Samy, G. N., Ahmad, R., & Ismail, Z. (2009). Threats to Health Information Security. In *2009 Fifth International Conference on Information Assurance and Security* (pp. 540–543). IEEE. doi:10.1109/IAS.2009.312

Spencer, L., Ritchie, J., Lewis, J., & Dillon, L. (2003). *Quality in Qualitative Evaluation: A Framework for Assessing Research Evidence*. Govt. Chief Social Researcher's Office.

Symantec. (2013). *Internet Security Threat Report 2013* (Vol. 18).