Indian Journal of Science and Technology, *Vol 9(42), DOI: 10.17485/ijst/2016/v9i42/100811, November 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Safety and Privacy Issues of Electronic Medical Records

Abdul Rahim Fiza[1,2*], Salahuddin Lizawati [1,3], Ismail Zuraini[1] and Samy Ganthan Narayana[1]

[1]Advanced Informatics School (AIS), University Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia; fiza2@live.utm.my, zurainiismail.kl@utm.my, ganthan.kl@utm.my

[2]College of Computer Science and Information Technology, University Tenaga Nasional (UNITEN), Kajang, Malaysia;

[3]Faculty of Information and Communication Technology, University Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia; lizawati22@live.utm.my

Abstract

Objectives: The objective of this study is to review the safety and privacy issues of electronic medical records (EMR). **Methods/Statistical Analysis**: Secondary sources from Springer Link, Science Direct, Emerald Library, IEEE Explorer Digital Library, Taylor & Francis Online, and EBSCO host databases were used to reviews relevance articles. **Findings:** Intersection and inter-reliant components of the healthcare system as well technology-induced errors were documented as the safety issues in the EMR implementation. Additionally, information sharing and access control were recognized as the important privacy issues. This information will be valuable in identifying what should be considered on the implementation of appropriate security measures in safeguarding EMR. **Application/Improvements:** This review can be useful towards protecting privacy and safe implementation of EMR.

Keywords: Electronic Medical, Healthcare Information System, Privacy, Review, Safety

Introduction

The growth of information system is discernible in most of organizations. In healthcare environment, a number of healthcare information systems (HIS) were developed to assist healthcare organizations to provide efficient and quality healthcare services. The massive development in healthcare technology has enabled the collection, storage, management, and sharing of electronic medical records (EMR) or interchangeably electronic health records (EHR)[1,2] among healthcare employees and other related healthcare institutions[3].

The innovation of HIS development has transformed the way healthcare employees managed the EMR. EMR is utilised by healthcare employees from various job backgrounds in a healthcare organisation, including healthcare practitioners, researchers, hospital administrators, and healthcare management personnel for specific reasons. Healthcare practitioners and researchers use EMR to improve diagnosis and treatment of diseases, while hospital administrators and healthcare management personnel use EMR to support their organization's services.

The use of EMR can lead to a safer care by improving communication among healthcare practitioners, and facilitating shared decision making[4]. Therefore, it must be performed in a way that addressed safety and privacy. Furthermore, EMR involve interaction between healthcare practitioner and complex sociotechnical system. Complex sociotechnical system involves multifaceted interaction among the people, technology, processes, organizations, and environment[5]. For instance, patient-care involves interrelated and collaborative work of multilevel healthcare practitioners such as doctors and nurses to treat and monitor patients. Communication and teamwork issues were found to be among the important contributing factors to adverse events in dynamic domains of healthcare[6].

*Author for correspondence

Additionally, the healthcare practitioners interact with technology such as HIS to assist their patient-care activities. Nevertheless, the adoption of HIS alters prior patterns of work, communication, or relationships among healthcare practitioners[7]. Moreover, the patient-care process is influenced by the environment and organization like interruptions, policies and procedures. Interruptions could lead to an error if the healthcare practitioners did not give adequate time and attention to complete the task properly[8]. For an example, interruptions resulted in healthcare practitioners to inadvertently enter the wrong order or the wrong patient into the HIS[9,10]. Thus, it may introduce new safety risks such as dosage errors, delay in detection of fatal illnesses, and delaying treatment. The safety risks can lead to safety incidents which could have resulted, or did result, in unnecessary harm to a patient[11]. Patient safety links to medical errors can be defined as the prevention of medical errors that could harm to patient[12,13]. Therefore, reducing medical errors and improving patient safety is the primary quality improvement focus in the healthcare environment[13,14].

Recent development in technology was found to have benefited the healthcare sector in reducing their operation cost and allowing the sharing of data with other stakeholders such as government agencies, health research institutes, insurance companies, and other healthcare institutions[15]. However, according to[16], several threats are involved when dealing with information sharing and privacy; for instance, involuntarily exposure of patients' identity by being anonymous and the selling of personal information for targeted advertising. Therefore, security and privacy conditions still remain as the main concern that must be scrutinised in an extensive way[17].

In protecting privacy, it is important for healthcare organisation to ensure the ability of HIS in preserving the security of EMR[18]. Healthcare employees must collect and communicate EMR securely, and do not disclose any sensitive information when EMR is being disseminated. Having privileged access to sensitive patient information, healthcare employees may lead to privacy breaches with potentially severe concerns. Thus, healthcare organisation should provide a proper mechanism in ensuring the privacy of sensitive data[19]. Since there are various types of potential privacy breaches such as theft, loss, unauthorized access/disclosure, improper disposal, fraud and hacking of confidential information, this may lead to detrimental consequences. To date, with the enacted Personal Data Protection Act (PDPA)[20], which include coverage for healthcare data implies that Malaysia legal environment has deemed healthcare sector as being in need of guidance with regard to patient privacy protection.

This study aims to review the safety and privacy issues of EMR. This paper is organized into five sections. The first section is introduction, followed by the research methodology. The third section describes the details about EMR. Then, the fourth section enlightens the findings in details from the review of safety and privacy issues of EMR. The last section summarizes the discussion.

Research Methodology

The review on safety and privacy issues in healthcare environment were based on secondary sources. The information obtained from journals, conference papers, industry reports, and books were summarized in developing the understanding on safety and privacy issues. The online databases that were given particular attention include: Springer Link, Science Direct, Emerald Library, IEEE Explorer Digital Library, Taylor & Francis Online, and EBSCO host.

Search terms used to find relevant articles included healthcare information systems, electronic medical records, electronic health records, safety, technology-induced errors, privacy, information sharing, and access control. The inclusion criteria for the articles were predetermined to be: 1) Articles published in English, 2) full-text articles, and 3) comprise of safety or privacy issues related to the HIS.

Tables contained key elements to be extracted from the selected articles were created. The key elements include author(s), title, journal, publication year, findings, and conclusion. Data from the selected articles that meet the aims of the study were then extracted and entered into the tables by the first and second author. The other review team independently evaluated the extracted data. The contradictions in the findings were resolved by discussing among the review team.

Electronic Medical Records

The upgrading of information technology into healthcare field shows the conversion of paper-based patients' medical records to electronic patients' medical records. This technology applied to various information

and communication technologies in healthcare organisation used to collect, transmit, display, or store patient data[21].

In recent years, a number of transformative technologies have developed in healthcare organisation in order to improve clinical outcomes, reducing cost, and improving patient safety. As new technologies such as HIS, computerized physician order entry (CPOE), online information portals, and clinical decision support systems (CDSS) are adopted by healthcare organisation.

In HIS, it is common for any healthcare employees to interact about EMR throughout the healthcare organisation. EMR can be denoted as a "personal information containing identification, history of medical diagnosis, digital renderings of medical images, treatments, medication history, dietary habits, sexual preference, genetic information, psychological profiles, employment history, income and physicians' subjective assessments of personality and mental state"[22].

EMR starts with creating or updating general record about patient by administrative clerk, a doctor would work out a diagnosis or treatment plan, and a nurse would complete their duties as instructed by the doctor. When these healthcare services are performed, healthcare employees are working on the relevant parts of the EMR based on their role in the healthcare organisation.

In replacing the difficulty of using paper-based medical records, EMR can be considered as a solution for integrating medical records from various departments and increase it accessibility. It also allows healthcare organisation to share the most recent information of EMR throughout the organisation.

The massive developments of mobile devices and web-based applications in healthcare field[23–25] also allow the users to improve the convenience of sharing the records throughout the organisation[26]. Despite of being processed by an autonomous device, EMR is stored, processed and transferred to several parties, such as doctors' offices, hospitals, pharmacy, and laboratories.

This study adapts definition of EMR based on[26] definitions;

"Electronic medical records (EMR) refer to personal information about patients used by healthcare employees to identify the right medical treatment and can be shared among individuals or groups in the healthcare organisation".

Safety and Privacy Issues

Safety Issues

Growing concerned related to errors resulted from the implementation and usage of HIS has increased[27]. A number of national initiatives has been taken to comprehend the safety of HIS[28,29]. Sociotechnical approach is frequently recommended for patient safety improvement efforts[30]. Safety incidents emerged from the interactions between people, and the elements of technologies, tasks, environment, and organisation in which they work in. Previous studies have confirmed that the antecedents towards safety use of HIS are influence by the sociotechnical aspect[31–35]. Certainly, it is essential to ensure the safety use of HIS. The implementation of HIS must look into from the perspective of sociotechnical approach. As such, this can provide further insights into safety implementation of HIS as a tool to improve quality of healthcare and patient safety.

(1) Intersection and Inter-reliant Components

Healthcare system is a complex and high-risk system[36]. The complex activities required ad hoc and pragmatic response that are never completely predictable of patients' reaction[37]. In critical care, the complexity of performing tasks is augmented by the constrictions of time, inadequate or unavailable information, by stress, and by repeated and unpredictable interruptions[38]. Besides, healthcare practitioners perform multiple task simultaneously such as interpreting physical signs and diagnostic tests, and bound with organizational policies and with the patient's personal needs[39]. Healthcare also involves intersection and inter-reliant components such as various level of professional from various departments with multiple viewpoints are required for a specific treatment. The tasks are frequently context-dependent, unpredictable, interrupted, and depend on coherent and timely communication between different healthcare practitioners[39]. Therefore, the interdependent natures facilitate the propagation of errors such that any error created by one component may affect other components as well which is normally unpredictable.

(2) Technology-induced Errors

Since the publication of the Institute of Medicine (IOM) report entitled "To Err Is Human: Building a Safer Health System", paramount attention has been given by

healthcare organizations and institutions at both national and international level to create a safety healthcare. In their report stated that 98,000 people die every twelve months in the United States (US) resulting from medical errors. Consequent to this report, the implementation of HIS has become a primary strategy to improve the safety of healthcare. Indeed, many developed countries such as the US, United Kingdom (UK), Australia, and Canada have proactively encouraged the implementation of HIS[40,41].

In addition to the evidence indicating that HIS can improve patient safety, there are growing evident indicating that the HIS seemed to foster errors rather than reducing the possibilities of errors. For instance, the US Food and Drug Administration (FDA) reported 42 reports of patient harm and four deaths in 436 critical incidents involving health information technology (IT) over a 30-month period[42]. In analyzed 456 safety incidents reported in a clinic at the University Hospital in Basel, discovered that medication errors was the most frequent type of safety incidents[43]. Majority of the safety incidents were caused by human errors, accounted for 56% and followed by communication problems, accounted for 26%. Similarly, 100 unique and closed investigations reported incidents were analyzed in a study conducted[44]. The study revealed 74 of the safety concerns involved unsafe technology, whereas 25 involved unsafe use of technology. From the three studies, it was found that poorly designed and usage of HIS resulting in endangering the patient with injury and death.

HIS introduces new classes of errors called technology-induced errors[45]. These errors are often not predictable at design, but recognized once HIS deployed in the real environment. In large complex systems, safety issues tend to arise from unexpected interactions between system components. The examples of errors are wrong input, data retrieval error and lack of data transmission[46]. The root cause of HIS related errors are complex and originate from variety of factors. It may be related to the technology itself, user behaviors, organisation, complex process and environment. Governments' and international bodies have put great deal of effort to find preventive mechanisms and solutions through investment in further analysis and regulation of systems. Hence, it is vital for all stakeholders involved in the development, implementation, and adoption of the HIS to be more cautious on the errors emerged from the HIS. Safety aspects should be one of the serious focuses in the HIS.

Privacy Issues

In healthcare organisation, the integration of EMR has drawn attention to privacy issues and threats. In claimed that the implementation and exchanging of EMR may formed privacy breaches and security violations[47]. Privacy breaches related with EMR remain as headlines in the media[48]. It may give serious implications for healthcare practitioners and their patients[49]. Furthermore, these breaches may give consequences on the healthcare organizations reputation, monetary fines, along with possible civil and criminal liabilities[50].

Most scholars agreed that if the record is related with medical information, there is a need to ensure the privacy of information[51–58]. Therefore, it is important for healthcare organisation to ensure their healthcare employees manage and treat EMR in a proper way with an appropriate security measures.

(1) Information Sharing

Healthcare practitioners, hospitals and insurers routinely use computers, phones, faxes, and other means or technologies to record, transfer and share information about patients. Healthcare organisation must ensure that the information are available when it is needed[59]. These information consist sensitive information related to health care records including identification, history of medical diagnoses, rendering of medical images, treatments, prescriptions, dietary habits, sexual preference, genetic information, psychological profiles, employment history, income, and insurance information[60].

Recent technology in healthcare industry was found to have benefited in reducing their operation cost and allowing the sharing of data with other stakeholders such as government agencies, health research institutes, insurance companies, and other healthcare institutions. However, 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 the insurance companies or other healthcare providers[61].

According to several threats are involved when dealing with information sharing and privacy; for instance, involuntarily exposure of patients' identity by being anonymous and the selling of personal information for targeted advertising. Since EMR are being used by various person-in-charge, departments, and organizations, it is also important to ensure the accuracy of data stored and processed[62]. In stated that policies should be apply to

all hardware and software available in the organization to safeguard the resources[63]. Hence, it is essential for healthcare organisation to give extra careful in implementing proper information sharing mechanism to protect privacy of EMR.

(2) Access Control

In a given situation where patients' sensitive information is not properly protected, anyone who walks by a fax machine or logs on to a computer may manipulate it for illegal purposes. This can be considered as privacy breach, whether those involving paper records which are susceptible to physical loss or acts of vandalism, or information stored in electronic form that could be misused in a number of ways[64]. Confidentiality is lost whenever an unauthorized party gains access to EMR. The exposure of EMR could result in the loss or denial of health insurance, job discrimination or personal embarrassment[65–67].

With the paper-based records, the accessibility of the data was restricted, and therefore, the information was less exposed and less vulnerable to information abuse. However, paper-based records could be easily misplaced or lost. These problems could be resolved with HIS development. In an effort to enhance the data accessibility, it could easily transformed into a threat when sensitive data consist in EMR would become easily accessible and vulnerable, which then leads to the main challenge in maintaining privacy of EMR[68–70]. With a number of users accessing EMR, managing access control becomes one of the main important privacy issue[71]. Hence, it is important for healthcare organisation to offer privacy guarantee at all levels within the system.

The control and access to HIS should be defined clearly to ensure that patients' privacy is not exposed to unauthorized parties[72]. Healthcare organisation must apply the need-to-know basis to the system users (including doctors, nurses, and administrative officers) when accessing EMR. This kind of restriction is supposed to protect EMR belong to specific units or departments in the organisation.

Thus, an advanced technological method should be applied as a solution to retrieve and exchange EMR in a secure and reliable way throughout the healthcare organisation. Healthcare organisation should establish rules to control authorization on their HIS resources and implement several types of authentication technologies such as multiple biometrics for identifying users before they are allowed access to HIS.

Conclusion

The review had successfully highlighted the key issues pertaining to the EMR. This review provides useful information and knowledge that both safety and privacy which are crucial issues in the implementation of EMR. The safety issues are concerned with the intersection and inter-reliant components of the healthcare system as well technology-induced errors resulting from the poorly designed and usage of HIS. On the other hand, the privacy issues are related to the information sharing and access control. Safety and privacy issues emerged from the implementation of EMR defeat its purpose to improve the quality of healthcare services. Therefore, the implementation of EMR should consider the complex interactions between socio and technical aspects exist in the healthcare setting as well appropriate security measures in retrieving and exchanging information through EMR.

Acknowledgements

This study is supported by Ministry of Higher Education (MOHE) Malaysia, University Teknikal Malaysia Melaka (UTeM) Malaysia and Zamalah Scholarship from University Teknologi Malaysia (UTM).

References

1. Baroody AJ, Hansen SW. Changing Perspective: Institutional Logics of Adoption and Use of Health Information Technology. Orlando: Thirty Third International Conference on Information Systems. 2012 Dec; p. 1-18.
2. Tiggle M. Urban Alabama Physicians and the Electronic Medical Record: A Qualitative Study. Dissertations/Theses - Doctoral Dissertations. 2012 Jul; p. 1-111.
3. Adler-Milstein J, Ashish KJ. Sharing Clinical Data Electronically: Critical Challenge for Fixing the Health Care System. J Am Med Assoc. 2012 Apr; 307(16):1695-96.
4. Health IT and Patient Safety: Building Safer Systems for Better Care. Date Accessed: 8/11/2011: Available from: http://www.nationalacademies.org/hmd/Reports/2011/Health-IT-and-Patient-Safety-Building-Safer-Systems-for-Better-Care.aspx.
5. Aarts J. Towards safe electronic health records: A socio-technical perspective and the need for incident reporting. Heal Policy Technol. 2012 Mar; 1(1):8-15.
6. Manser T. Teamwork and patient safety in dynamic domains of healthcare: a review of the literature. Acta Anaesthesiol Scand. 2009 Feb; 53(2):143-51.

7. Harrison MI, Koppel R, Shirly BL. Unintended Consequences of Information Technologies in Health Care — An Interactive Sociotechnical Analysis. J Am Med informatics Assoc. 2007 Sep-Oct; 14(5):542-49.
8. Slight S, Howard R, Ghaleb M. The causes of prescribing errors in English general practices: a qualitative study. Br J Gen Pract. 2013 Oct; 63(615):e713-20.
9. Farley HL, Baumlin KM, Hamedani AG. Quality and safety implications of emergency department information systems. Ann Emerg Med. 2011 Oct; 62(4):399-407.
10. Salahuddin L, Ismail Z. Safety Use of Hospital Information Systems: A Preliminary Investigation. Knowledge Management in Organizations. Springer International Publishing. 2015 Aug; p. 707-21.
11. Runciman W, Hibbert P, Thomson R, Van Der Schaaf T, Sherman H, Lewalle P. Towards an International Classification for Patient Safety: key concepts and terms. Int J Qual Health Care. 2009; 21(1):18-26. DOI: 10.1093/intqhc/mzn057.
12. Aspden P, Corrigan JM, Wolcott J, Erickson SM. National Academies Press: Patient Safety: Achieving a New Standard for Care. 2004.
13. Kohn LT, Corrigan JM, Molla S. National Academies Press: To Err Is Human: Building a Safer Health System. 2000.
14. Crossing the Quality Chasm: A New Health System for the 21st Century. Date Accessed: 03/2001: Available from: file:///C:/Users/laptop/Downloads/reportbrief.pdf.
15. AbuKhousa E, Mohamed N, Al-Jaroodi J. e-Health Cloud: Opportunities and Challenges. Futur Internet. 2012 Jul; 4:621-45.
16. Kaletsch A, Sunyaev A. Privacy Engineering: Personal Health Records in Cloud Computing Environments. Shanghai: Thirty Second International Conference on Information Systems. 2011; p. 1-11.
17. Ermakova T, Erek K, Huenges J. Cloud Computing in Healthcare – a Literature Review on Current State of Research. Chicago, Illinois: Proceedings of the Nineteenth Americas Conference on Information Systems. 2013 May; p. 1-9.
18. Monem H, Hussin ARC, Sharifian R, Shaterzadeh H. CRM software implementation factors in hospital: Software & patient perspectives. 2011 5th Malaysian Conf Softw Eng MySE. 2011 Dec; p. 159-64.
19. Abdul Rahim F, Ismail Z, Samy GN. Information Privacy Concerns in Electronic Healthcare Records: A Systematic Literature Review. 2013 International Conference on Research and Innovation in Information Systems (ICRIIS). 2013 Nov; p. 504-9.
20. Laws of Malaysia Act 709. Date Accessed:10/06/2010: Available from: http://www.kkmm.gov.my/pdf/Personal%20Data%20Protection%20Act%202010.pdf.
21. Sittig D, Singh H. Defining health information technology–related errors: New developments since To Err Is Human. Arch Intern Med. 2011 Jul; 171(14):1281-84.
22. Mercuri RT. The HIPAA-potamus in health care data security. Commun ACM. 2004 Jul; 47(7):25-8.
23. Haakon Bryhni JM, Ruland CM. Secure Solution for Mobile Access to Patient's Health Care Record. IEEE 13th Int Conf e-Health Networking, Appl Serv. 2011 Jun; p. 296-303.
24. Mancini F, Gejibo S, Mughal KA, Valvik RAB, Klungsoyr J. Secure Mobile Data Collection Systems for Low-Budget Settings. 2012 Seventh Int Conf Availability, Reliab Secur. 2012; p. 196-205.
25. Cubic I, Markota I, Benc I. Application of Session Initiation Protocol in Mobile Health Systems. 33rd Int Conv Inf Commun Technol Electron Microelectron. 2010 May; p. 367-71.
26. Sandıkkaya MT, Decker B De, Naessens V. Springer Berlin Heidelberg: Privacy in Commercial Medical Storage Systems. Szomszor M, Kostkova P, eds. Electronic Healthcare. 2012; p. 247-58.
27. Beuscart-Zephir MC, Borycki EM, Carayon P, Jaspers MWM, Pelayo S. Evolution of human factors research and studies of health information technologies: the role of patient safety. Yearb Med Inform. 2013; 8(1):67-77.
28. Kushniruk AW, Bates DW, Bainbridge M, Househ MS, Borycki EM. National efforts to improve health information system safety in Canada, the United States of America and England. Int J Med Inform. 2013 May; 82(5):e149-60.
29. Magrabi F, Aarts J, Nohr C. A comparative review of patient safety initiatives for national health information technology. Int J Med Inform. 2013 May; 82(5):e139-48.
30. Middleton B, Bloomrosen M, Dente MA. Enhancing patient safety and quality of care by improving the usability of electronic health record systems: recommendations from AMIA. J Am Med Inform Assoc. 2013 Jun; 20(e1):e2-e8.
31. Salahuddin L, Ismail Z. Antecedents for Safety in Health IT : An Exploratory Investigation. Putrajaya: IEEE, Information Technology and Multimedia (ICIMU). 2014 Nov; p. 38-43.
32. Odukoya OK, Chui MA. E-prescribing: a focused review and new approach to addressing safety in pharmacies and primary care. Res Social Adm Pharm. 2013 Nov-Dec; 9(6):996-1003.
33. Harrington L, Kennedy D, Johnson C. Safety Issues Related to the Electronic Medical Record (EMR): Synthesis of the Literature from the Last Decade. J Healthc Manag. 2011 Jan; 56(1):31-43.
34. Frith KH. Medication errors in the intensive care unit: literature review using the SEIPS model. AACN Adv Crit Care. 2013 Oct-Dec; 24(4):389-404.
35. Salahuddin L, Ismail Z. Classification of antecedents towards safety use of health information technology: A systematic review. Int J Med Inform. 2015 Nov; 84(11):877-91.
36. Taib IA, McIntosh AS, Caponecchia C, Baysari MT. A review of medical error taxonomies: A human factors perspective. Saf Sci. 2011 Jun; 49(5):607-15.

37. Berg M. Patient care information systems and health care work : a sociotechnical approach. Int J Med Inform. 1999 Aug; 55(2):87-101.
38. Alvarez G, Coiera E. Interruptive communication patterns in the intensive care unit ward round. Int J Med Inform. 2005 Oct; 74(10):779-81.
39. Ash JS, Berg M, Coiera E. Some Unintended Consequences of Information Technology in Health Care : The Nature of Patient Care Information System-related Errors. J Am Med Informatics Assoc. 2004 Mar-Apr; 11(2):104-12.
40. Morrison Z, Robertson A, Cresswell K, Crowe S, Sheikh A. Understanding contrasting approaches to nationwide implementations of electronic health record systems: England, the USA and Australia. J Healthc Eng. 2011 Mar; 2(1):25-42.
41. Rozenblum R, Jang Y, Zimlichman E. A qualitative study of Canada's experience with the implementation of electronic health information technology. Can Med Assoc J. 2011 Mar; 183(5):E281-88.
42. Magrabi F, Ong M-S, Runciman W, Coiera E. An analysis of computer-related patient safety incidents to inform the development of a classification. J Am Med Inform Assoc. 2010 Nov-Dec; 17(6):663-70.
43. Scharein P, Trendelenburg M. Critical incidents in a tertiary care clinic for internal medicine. BMC Res Notes. 2013 Jul; 6:276.
44. Meeks DW, Smith MW, Taylor L, Sittig DF, Scott JM, Singh H. An analysis of electronic health record-related patient safety concerns. J Am Med Informatics Assoc. 2014 Nov-Dec; 21(6):1053-59.
45. Kushniruk AW, Triola MM, Borycki EM, Stein B, Kannry JL. Technology induced error and usability: the relationship between usability problems and prescription errors when using a handheld application. Int J Med Inform. 2005 Aug; 74(7-8):519-26.
46. Magrabi F, Ong MS, Runciman W, Coiera E. Using FDA reports to inform a classification for health information technology safety problems. J Am Med Inform Assoc. 2012 Jan-Feb; 19(1):45-53.
47. Aidemark Jan. Knowledge Management Paradoxes. The Electronic Journal of Knowledge Management. 2009; 7(1):1-10.
48. Hodgkinson R, Branz L, Culnan M, Dhillon G, MacWilson A. Information Security and Privacy: Rethinking Governance Models. International Conference on Information Systems (ICIS). 2010 Jan; p. 1-5.
49. Abdul Rahim F, Ismail Z, Samy GN. Information Privacy Concerns in the Use of Social Media Among Healthcare Practitioners: A Systematic Literature Review. Adv Sci Lett. 2014 Oct; 20(10):2176-79.
50. Culnan MJ, Williams CC. How Ethics Can Enhance Organizational Privacy: Lessons from the Choice Point and TJX Data Breaches. MIS Q. 2009 Dec; 33(4):673-87.
51. Appari A, Johnson ME. Information security and privacy in healthcare: current state of research. Int J Internet Enterp Manag. 2010; 6(4):279-314.
52. London School of Economics and Political Science. Date Accessed: 7/07/2016: Available from: http://www.lse.ac.uk/home.aspx.
53. Randolph C, Barrows JR, Clayton PD. Privacy, Confidentiality and Electronic Medical Records. J Am Med Informatics Assoc. 1996 Mar-Apr; 3(2):139-48.
54. Kurtz G. EMR Confidentiality and Information Security. J Healthc Inf Manag. 2002; 17(3):41-8.
55. Lee LM, Gostin LO. Ethical Collection, Storage, and Use of Public Health Data: A Proposal for a National Privacy Protection. J Am Med Assoc. 2009 Jul; 302(1):82-4.
56. Hall MA, Schulman KA. Ownership of Medical Information. J Am Med Assoc. 2009 Mar; 301(12):1282-84.
57. Simon SR, Evans JS, Benjamin A, Delano D, Bates DW. Patients attitudes toward electronic health information exchange: qualitative study. J Med Internet Res. 2009 Jul-Sep; 11(3):e30.
58. Carrion Senor I, Fernandez-Aleman JL, Toval A. Are personal health records safe? A review of free web-accessible personal health record privacy policies. J Med Internet Res. 2012 Aug; l4(4):e114.
59. Hassan NH, Ismail Z, Rahim FA. A Review on Barriers in Adopting Healthcare Information System. Adv Sci Lett. 2014 Jan; 20(10-12):2184-87.
60. Anton AI, Earp JB, Reese A. Analyzing Website Privacy Requirements Using a Privacy Goal Taxonomy. IEEE Joint International Requirements Engineering Conference. 2002; p. 23-31.
61. Hasan O, Habegger B, Brunie L, Bennani N, Damiani E. A Discussion of Privacy Challenges in User Profiling with Big Data Techniques: The EEXCESS Use Case. Santa Clara, CA: IEEE, 2013 IEEE International Congress on Big Data. 2013; p. 25-30.
62. Abdul Rahim F, Ismail Z, Samy GN. Information Privacy Concerns in Electronic Medical Records: A Preliminary Investigation. Knowledge Management in Organizations Lecture Notes in Business Information Processing. 2014 Sep; p. 177-85.
63. Sarkheyli A, Alias RA, Ithnin N. A Conceptual Formative Framework of Knowledge Risk Governance to Enhance Knowledge Sharing. PACIS 2014 Proceedings. 2014; p. 1-12.
64. Grunwell D, Gajanayake R, Sahama T. Demonstrating Accountable-eHealth Systems. 2014 IEEE International Conference on Communications (ICC). 2014 Jun; p. 4258-63.
65. Spector N, Kappel DM. Guidelines for Using Electronic and Social Media : The Regulatory Perspective. Online J Issues Nurs. 2012 Sep; 17(3):1.
66. Cushman R, Froomkin AM, Cava A, Abril P, Goodman KW. Ethical, legal and social issues for personal health records and applications. J Biomed Inform. 2010 Oct; 43(S5):S51-S55.

67. Nass SJ, Levit LA, Gostin LO. Beyond the HIPAA Privacy Rule: Enhancing Privacy. Improving Health Through Research. 2009.
68. Fong S, Zhuang Y. Using medical history embedded in biometrics medical card for user identity authentication: privacy preserving authentication model by features matching. J Bomedicine Biotechnol. 2012; 2012:1-11.
69. Kumar S, Nilsen WJ, Abernethy A. Mobile health technology evaluation: the mHealth evidence workshop. Am J Prev Med. 2013 Aug; 45(2):228-36.
70. Nageba E, Defude B, Morvan F. Data Privacy Preservation in Telemedicine : The PAIRSE Project. Stud Health Technol Inform. 2011; 169:661-65.
71. Abdul Rahim F, Ismail Z, Samy GN. Security Issues in Electronic Health Record. Open Int J Informatics. 2013; 1:59-68.
72. Guo R, Wen Q, Jin Z, Zhang H. An efficient and secure certificateless authentication protocol for healthcare system on wireless medical sensor networks. Scientific World Journal. 2013 Apr; 2013:1-7.