Journal of Theoretical and Applied Information Technology
31st August 2016. Vol.90. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SYSTEMATIC REVIEW ON DATA SECURITY AND PATIENT PRIVACY ISSUES IN ELECTRONIC MEDICAL RECORDS

[1]AMJAD MAHFUTH, [2]JASPALJEET SINGH DHILLON AND [3]SULFEEZA MOHD DRUS

[1] lecturer, Department of Information Systems, Alquds Open Univeristy, Tulakrm, Palestine.
[2] Dr., Department of Information Systems, Universiti Tenaga National, Selangor, Malaysia
[3]Dr., Department of Information Systems, Universiti Tenaga National, Selangor, Malaysia
E-Mail: [1]amahfouth99@gmail.com, [2]jaspaljeet@gmail.com, [3] sulfeeza@uniten.edu.my

ABSTRACT

The adoption of Electronic Medical Records (EMR) in healthcare organizations has numerous benefits to physicians, patients, and healthcare services. However, unresolved security and privacy concerns pertaining to patient information cause relatively low adoption of EMR by health institutions. Safeguarding large amount of sensitive health data at different locations and forms proves to be a major challenge of EMR. In this paper, a Systematic Literature Review (SLR) is presented to (1) identify the security and privacy concerns in the adoption of EMR by health organizations and (2) to analyze the existing solutions in addressing the identified concerns. A total of 393 papers were found in this regard. After careful study and the removal of duplicate papers and screening of studies, 15 papers which met the inclusion criteria were selected for the review. This review will help researchers to be aware of the privacy and security concerns of EMR and the existing solutions. The review revealed that the security and privacy issues related to EMR are inadequately addressed. This study indicates that the technical and financial supports are insufficient to overcome the security issues of EMR, and thus, the success factors and security culture should be investigated. Developing countries meet many challenges in adopting EMR, especially due to the lack of security policy and background infrastructure. Hence, novel solutions such as best practice guidelines with respect to security and privacy are necessary to aid successfully adoption EMR.

Keywords: *Electronic medical record, security policy, privacy, systematic review.*

1. INTRODUCTION

In the last decade, Information Technology has played a prominent role in the field of healthcare. The continuous development in the communications technology in the healthcare sector has led to a new concept called e-health, which refers to any electronic exchange of health-related data collected or analyzed through an electronic connectivity for improving efficiency and effectiveness of healthcare delivery [1, 2]. This new generation of healthcare sector provides electronic utilities and tools to stakeholders and clinicians in executing their duties electronically, instead of using papers and related traditional utilities.

One of the most important records in the concept of e-health is Electronic Medical Record (EMR). EMR is a digital version of a paper chart that contains all of a patient's medical history maintained by a health organization and is used by providers for diagnosis and treatment. EMR contains patient data such as the patient history, diagnosis, treatments, radiology, laboratory and ward booking [3]. All of these pieces of information are kept electronically in physical storage devices in the hospital databases or in any other extra storage available such as the clouding storage, or web services. One of the main issues related to EMR is patients' privacy and information security from hacking, abuse, or misuse that will absolutely affect the integrity, quality and availability of EMR data [4]. In fact, EMR is critical and sensitive for healthcare service environments since it involves a large volume of patient information that is stored in the storage devices.

On one hand, the adoption of health technologies in healthcare services such as EMR has the potential to improve the coordination of care, healthcare quality, patient engagement, and many other areas of healthcare [5]. On the other hand, we cannot ignore the challenges, especially the issues related to the privacy and the information security of the stored data in EMR that prevents the system from being fairly used and adopted by healthcare services [6]. Hence, the widespread

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

usage of EMR is still at an early stage and adoption in developing countries [4, 6]. Understanding the security as well as the privacy issues is the key challenge with regard to the adoption of EMR. In general, healthcare services are keen to leverage EMR but with the reservation in the privacy of the patient information and information security.

In EMR, patients are expected to share their personal health data among physicians and sometimes between different healthcare services. However, they may decline on revealing important information as the disclosure of some information may result in social stigma and discrimination [7]. In addition, as mentioned, the adoption of EMR in healthcare services deals with a large amount of patient information and the health services information security has become critical for concerned stakeholders. Security policy and privacy issues are crucial for the EMR domain to keep its availability, integrity and it also helps to promote the quality of services. One of the most crucial barriers of EMR adoption is the concerns surrounding the privacy concept and security. It is important to understand how EMR is protected and what factors lead to the enhancement of a successful
e-health system.

In this paper, we identify the security and privacy concerns in the adoption of EMR by healthcare organizations and services, and analyze existing solutions in addressing the identified concerns.

This paper adopts the Systematic Literature Review (SLR) approach and is organised as follows. The first section describes the method we used in conducting the SLR. The subsequent section reports the results obtained based on the synthesis of the existing evidence. The next section discusses the key findings and implications of the review. The conclusion section is inclusive of both summary and future work.

2. METHODS

The SLR approach has been used in this paper to perform the research systematically and to reduce uncertainties and biases. We applied the basic SLR method as described by [8]. For this study, published papers were searched from four relevant databases IEEE Xplore, ACM digital library, Science Direct and Scopus and others databases (such as Google Scholar and Google search engine). The search was carried out between June 2015 and August 2015 using the following key words: [(security OR Security Policy OR Information Security OR Privacy OR Privacy issue OR security policy and Privacy issue OR protect OR Security challenges) AND (EMR OR electronic medical record OR E-health OR E-health Records) AND (Adoption OR barriers OR factors OR successes)].

The inclusion criteria for this search were: (1) any proposed security framework model for EMR or security policy of EMR or the security information system theories which are related to EMR, (2) any studies that present and analyze the security and privacy challenges of the adoption of EMR, (3) any articles which present the experimental adoption of EMR in developed and developing countries, (4) any articles which present the success factors of the security policy to protect EMR, and (5) any articles that focus on the problem gap regarding the security policy and privacy issues of EMR. The exclusion criteria were: (1) papers focusing on Electronic Health Records (EHR), (2) articles that focus on e-health in general, (3) articles not written in English, and (4) articles not specifically focusing on the security policy and privacy of EMR.

By applying the search in different databases, 393 papers were selected by looking at the titles: 92 papers were derived from IEEE Xplore, 114 papers were derived from the ACM digital library, 50 papers were derived from Scopus, 97 papers were derived from Science Direct journal and another 40 papers were derived from other resources. From these, 15 papers were found to be duplicates and they were removed accordingly. Of the remaining 378 papers, 220 were excluded because they did not meet the selection criteria, based on the content of their titles and abstracts. Examining the remaining 158 papers by looking first at the introduction, subsequently the headings and finally the conclusion for e-health cloud or/and web services applications or/and papers lacking fresh empirical data, resulted in 77 papers being left after the elimination process. From the list, papers which did not discuss effective security framework model and/or information security theory or/and factors which influence the security model of EMR and review papers were eliminated too. After exhaustive elimination, 15 papers were selected for the review. Figure-1 below shows the SLR flow diagram.

3. RESULTS

The study includes fifteen articles that have considered a relation to the title of this paper, and important information that was extracted from the reviewed papers (i.e. methodology and the significant finding of the article) is summarized in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table-1. From the table, it is noted that there were ten studies which focused on the security policy and privacy issues to protect EMR information from misuse, abuse, and keep EMR available, and confidential for physicians and staff. Of the ten studies, two studies provide the security framework model to secure EMR, three studies focused on the barriers and challenges to accept EMR in healthcare services, and two studies focused on the success factors which enhance the security of EMR.

The first objective of the review was to identify the security and privacy concerns in the adoption of EMR by healthcare organizations and services. Based on the findings of the review, healthcare organizations in the world are in the process of implementing and adopting EMR in their hospitals and health services. One of the most crucial challenges of adopting EMR is maintaining patient record information security. This is due to the fact that a large amount of information is related to patients as a result of the adoption of EMR. Physicians are to make medical decisions to treat individual patients based on patients' health records. Patients have concerns stemming from the disclosure of their information as EMR can be accessed by unauthorized persons. Therefore, the security policy and privacy issues of EMR are crucial to ensure that EMR record is accepted in healthcare services. Based on the findings, we define and focus on the problem gap related to the security policy and privacy issues of accepting EMR. The main issue of EMR is shown to protect EMR from unauthorized users in order to achieve the security requirements. The use of EMR allows accessibility to patient records from different locations and this increases the concern of information security, probably violating the patients' privacy. The privacy and confidentiality are two important issues for the patient information, i.e. any breaches of privacy and confidentially can result into major challenges to the health services. The existing solutions depend on the current infrastructure and the technical issue of the healthcare organization in specific countries such as developed countries, but on the other side it is necessary to find suitable solutions in developing the country, which meets a lot of challenges in the adoption of EMR and the lack of technology basics.

The second objective of the review was to analyze the existing solutions in addressing the concerns that have been identified. Based on the findings, there are multiple security concerns as presented on the first objective. The studies argued and provided security policies or techniques and security frameworks as a solution to protect EMR from hacking, misuse, and abuse. The existing solutions depend on the existing infrastructure and the technical issue of the healthcare organization in specific countries such as developed countries, but on the other side it is necessary to find some suitable solutions compatible with the requirements in developing countries and the lack of technology basics. Obviously, it is clear from the findings that developing countries have currently proceeded with the adoption of EMR without any serious consideration for the security policy to protect EMR. These countries have lack of security awareness, and security culture. They also suffer from the lack of technical and infrastructure backgrounds, as well as lack the enactment of ethics laws and rules to protect EMR and enhance the issue of privacy.

4. DISCUSSION

The adoption of EMR leads to large amount of sensitive patient information (e.g. medical history, allergies, and current treatments) accessible to physicians, authorized users as well as opportunists. The transmission of health data via the EHR between different branches of the same healthcare organization (or a different healthcare organization) could expose the records to opportunists (e.g. hackers) [25]. EMR allows accessibility to patient records from different locations, and this increases the security of information, probably violating the patient's privacy. Patients are encouraged to share their information between physicians and different healthcare services, and this actually means that the privacy of patient information is also violated [7].

Based on our review the existing security and privacy solutions are insufficient to maintain the patient privacy in EMR and to secure EMR from unauthorized user. The existing solutions enhance the security but it is not enough to keep the privacy and security of EMR together. Most of proposed solutions in this study indicated the physical technical and security factors as a solution to protect EMR and indicated the barriers meet the implementation process of EMR. Other studies argued the challenges of EMR implantation process in developing countries. The technical and financial supports as a security solution are not sufficient to overcome the security issues of EMR. In order to provide efficient security and privacy for EMR, we need to indicate and propose a security framework that promotes security policy as a technique to protect the patients' information, and provides strategies or plans to keep the patient privacy under the healthcare organizations. The proposed solution

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

is to integrate between the privacy issue, security policy and the factors which effect on them. Still there are many keys constrains and challenges in adoption of EMR, including privacy and security issues.

The continuous use of EMR has a significant impact on healthcare organizations and e-health globally. We noted that there are contradictory claims from physicians on the use of EMR. Some physicians claim that the adoption of EMR will achieve the efficiency of healthcare services provided by a health institution, while others claim that the adoption of EMR will expose the patient privacy that will lead into the breach of data security. Regardless of the claims, it is apparent that most healthcare organizations lead to a consensus to adopt EMR in addressing the pressing needs to maintain an accessible medical record of patients. The advantages of leveraging EMR override the disadvantages greatly. Therefore, it is essential to revise the existing security policies and patient privacy strategies in protecting EMR in healthcare organizations and the physicians should be adapted and learned.

The security policy has some great and effective advantages with regard to the availability and integrity of EMR to authorized users. Providing the security improve and promotion quality of the organization services, keep availability of data, keep integrity of data and protect the data itself from misuse, abuse, and from unauthorized modification as presented by [22-24].

Based on our review of existing studies related to EMR, we argued that developing countries lack necessary infrastructure, IT support, and security culture to implement EMR successfully as presented by [21, 17] and they argued that is one of the most striking barriers is the security and privacy of EMR. In a broad sense, we note that developing countries (e.g. Palestine) adopt EMR without any consideration of how to maintain data security and protect patient privacy, especially, in the absence of the laws. Therefore, our review signifies that there is lack of studies that provide the necessary guideline in the implementation of EMR, especially, in the areas of data security and patient privacy in developing countries.

The findings of included studies as discussed above are summarized below:

- Adoption of EMR leads to a large amount of health information which shared between physicians and different healthcare organizations.
- The use of EMR allows accessibility to patient records from different locations and this increases the concern of information security, probably violating the patients' privacy.
- The existing security and privacy solutions are insufficient to maintain the patient privacy in EMR and to secure EMR from unauthorized access.
- The existing solutions could technically enhance the security aspect of EMR but they are not effective to address both the privacy and security of EMR completely.
- Developing countries are lack of necessary infrastructure, IT support, and security culture to implement EMR effectively.

5. CONCLUSION AND FUTURE WORK

Although there are more advantages over disadvantages of adopting EMR in a healthcare institution, the adoption rate is relatively low and is often associated with inadequate addressing of security and patient privacy concerns. We have reviewed 15 recent studies to identify the security and privacy concerns in the adoption of EMR by health organizations and to analyze existing solutions in addressing the identified concerns. The study emphasized the importance of having a security policy and privacy issue to protect EMR in healthcare services, especially in developing countries.

The findings of this SLR will be useful to healthcare stakeholders (of developing countries like Palestine) in obtaining an overview about the barriers pertaining to the security policy and privacy concerns from the adoption of EMR, and for informers to develop novel security solutions (e.g. security and privacy framework) to address the issues. The study indicates that the technical and financial support is not sufficient to overcome the security issues of EMR. As suggested in this study, to overcome the challenges in accepting EMR, the physicians should be adapted and learned. Healthcare organizations should push the success factors as a positive influence in adopting safe EMR and proposing for some practical security framework solutions in order to promote the security policy and privacy issue in EMR.

Based on our review, the researchers should provide some in-depth techniques and different solutions to protect EMR from any concerns, and that said, the security is very important to protect EMR information and keep the privacy of patients.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

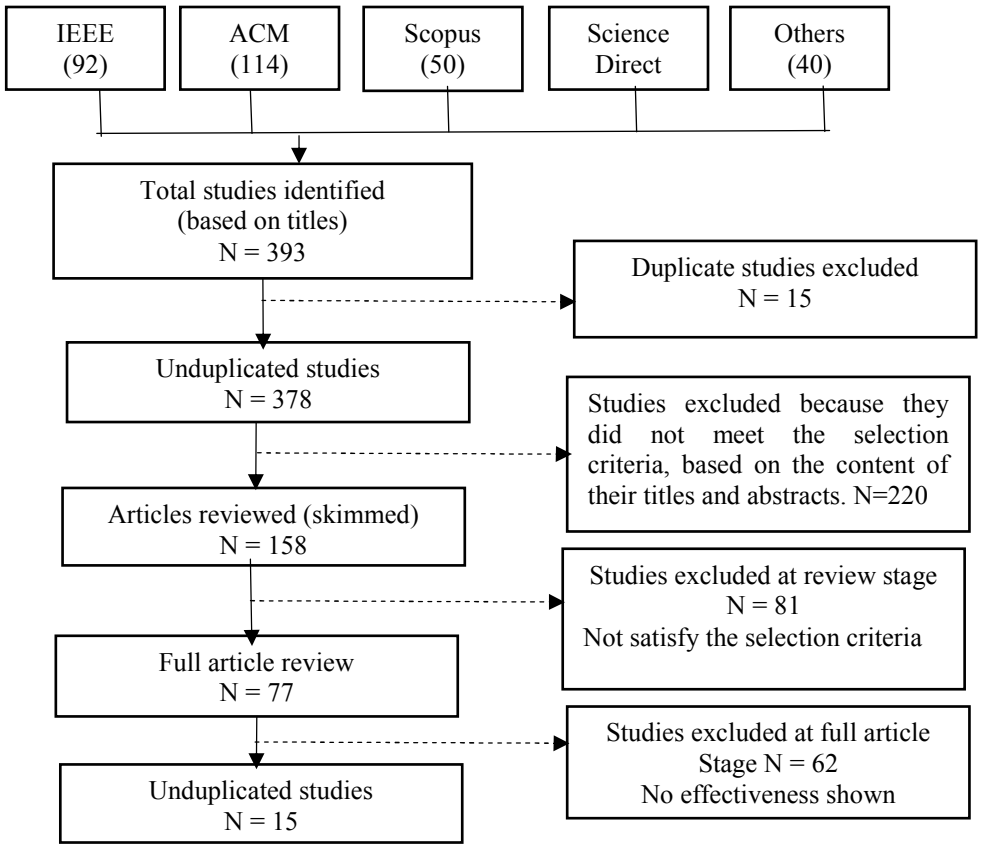

Figure-1. SLR Flow Diagram.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table-1. Analysis of the included studies.

No	Title	Methodology	Significant Findings
1.	Security of electronic medical information and patient privacy: What you need to know [4]	Survey	This paper provides some basic tools and techniques used to maintain medical information security and patient privacy that includes physical safeguards, technical safeguards, and administrative safeguards.
2.	Self-Protecting Electronic Medical Records Using Attribute-Based Encryption [9]	Survey	Design and implementation of self-protecting electronic medical records (EMRs) using attribute-based encryption are presented in this survey.
3.	Barriers to the acceptance of electronic medical Records by physicians from systematic review to taxonomy and interventions [10]	Survey	The barriers concerning the implementation of EMR have been identified. This survey conclude that the process of EMR implementation should be treated as a change project. The authors classified the barriers to eight categories, and they are: A) Financial, B) Technical, C) Time, D) Psychological, E) Social, F) Legal, G) Organizational, and H) Change Process.
4.	Overcoming challenges to use the Electronic Medical Records System (EMRs) in Jordan Hospitals [11]	Case study	This article discusses the factors which are recognized to be the challenges in the implementations of EMR in Jordanian hospitals.
5.	Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance [12]	Survey	The importance of the privacy of EMR and the patients' rights were discussed in this paper. In addition, cryptography algorithms and security requirements have been discussed.
6.	Electronic Records Handbook [13]	Survey	This article provides the backgrounds and the details of E-Record which representative with EMR, EHR, also it discussed the E-Record regulations, and the very familiar E-record.
7.	Electronic Medical Records : Success Requires an Information Security Culture [14]	Survey	Security culture as a success factor solution for EMR security to be in place with a holistic back-to-basics safety approach of the entire data lifecycle.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

8.	A Proposed Layered Architecture to Maintain Privacy Issues in Electronic Medical Records [15]	Security Framework Model	A novel architecture model for EMR, and provides the architecture to maintain the privacy of patients, finally the author proposed the factors layer to help maintain the data privacy in the EMR system.
9.	Factors Affecting Electronic Medical Record Acceptance by Specialist Physicians [16]	Questionnaire	This paper investigated the factors affecting EMR acceptance by specialists in Iran. The questionnaires posed questions based on eight main categories of barriers namely: financial, technical, time, psychological, social, legal, organizational, and change process. The most important barrier factors of EMR in this study were technical barriers such as the limitation of the system 96 (72.2%) and the interconnectivity/standardization 96 (72.2%) and the social factor of uncertainty about vendor 97 (72.9%), mentioned by the majority of physicians.
10.	Electronic Patient Record Security Policy in Saudi Arabia National Health Services [17]	Mixed Method	Security and privacy are the most challenging in adopting of EMR in Saudi Arabia, the key findings show that the Saudi Arabia EPR adoption process is currently proceeding without serious consideration for security policy to protect the Electronic Patient Record and a lack of awareness amongst the hospital staff.
11.	Evaluating E-health Services and Patients Requirements in Jordanian hospitals [18]	Questionnaire	The main challenge in accepting EMR in Jordan.
12.	Security Challenges and Success Factors of the Electronic Healthcare system [6]	Survey	This paper explored and analyzed the current state of e-health systems security and privacy of patient records to protect electronic patient records.
13.	Barriers to the Adoption of Health Information Technology in Arab Countries' Hospitals: Practitioners' Perspectives [15]	Mixed Method	The main barriers of adopting EMR in Arabic countries have been discussed such as lack of financial resources and high cost; poor management and bureaucracy; poor staff IT competency; lack of qualified IT personnel and lack of awareness of the Health IT value.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

14.	A Criticism of the Current Security, Privacy and Accountability Issues in Electronic Health Records [19]	Survey	The main challenges of EMR, EHR implementations such as security, privacy and the accountability were discussed, also they provide a possible solution subject to these challenges likes patient awareness as a factor of managing e-health records, the Encryption mechanism for protecting the record, also they provide a challenge of not providing patients' right and how the system can pinpoint the person who broadcasts medical records for accountability responsibility.
15.	Security and Privacy Issues in Healthcare Information System [20]	Survey	This paper discussed the difference between the security and privacy issues in the healthcare information system. The author suggested for the pseudonymization-based technique to be more suitable for the healthcare information system.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFRENCES:

[1] M. Cashen, P. Dykes and B. Gerber. 2004. E-Health Technology and Internet Resources :Barriers for Vulnerable Populations, Journal of Cardiovascular NursingVol. 19, No. 3, pp 209–214 | © 2004 Lippincott Williams & Wilkins, Inc.

[2] T. Kind and T. Silber. 2004. Ethical issues in pediatric e-health. Clinical Pediatrics,43(7),593-599.

[3] Terry. 2009. The Government Push for Electronic Medical Records, Medscape Family Medicine,

[4] K. P. Andriole .2014. Security of Electronic Medical Information and Patient Privacy: What You Need to Know, American College of Radiology,1546-1440/14/$36.00,

[5] C. Kelly and H. Rima. 2012. Patients want granular privacy control over health information in electronic medical records. Copyright 2012 by American Medical Informatics Association.

[6] G. Arash and Z. Shukur. 2013. The 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013), Security Challenges and Success Factors of Electronic Healthcare System", 2212-0173 © 2013 The Authors. Published by Elsevier Ltd. Open access under CC BY-NC-ND license. Selection and peer-review under responsibility of the Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia.

[7] D. Daglish and N. Archer. 2009. Electronic Personal Health Record System: A Brief Review of Privacy, Security, and Architectural Issues. Word Congress on Privacy, Security, Trust and the Management of e-Business, 2009. DE Groote School of Business. McMaster University.

[8] B.A. Kitchenham and S. Charters. 2007. Guidelines for Performing Systematic Literature Reviews in Software Engineering Technical Report EBSE-2007-01, 2007.

[9] J.A. Akinyele, L.U. Christoph, G.D. Matthew, W. Matthew, J.N. Zachary and D. Rubin. 2011. Self-Protecting Electronic Medical Records Using Attribute-Based Encryption.

[10] A. Boonstra and M. Broekhuis. 2010. Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions, Boonstra and Broekhuis BMC Health Services Research. 2010, 10:231 http://www.biomedcentral.com/1472-6963/10/231.

[11] Y.A. AL-nassar, A.M. Mohd and O. S. Wan. 2011. Overcoming challenges to use Electronic Medical Records System (EMRs) in Jordan Hospitals, IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.8, August 2011.

[12] O.H. Jalab, A. Hamid, A. M. Gazi, B. B. Zaidan and A.A. Zaidan. 2010. Securing electronic medical records transmissions over unsecured communications: An overview for better medical governance, Journal of Medicinal Plants Research Vol. 4(19), pp. 2059-2074, 4 October, 2010. Available on line at http://www.academicjournals.org /JMPR
ISSN 1996-0875 ©2010 Academic Journals

[13] Canadian Medical Protective Association. 2014. Electronic Records Handbook, This document is available on our website at cmpa-acpm.ca. Electronic Records Handbook.

[14] Thomas and Advisor. 2012. Electronic Medical Records: Success Requires an Information Security Culture.

[15] A. Bensefia and A. Zarrad. 2014. A Proposed Layered Architecture to Maintain Privacy Issues in Electronic Medical Records, E-Health Telecommunication Systems and Networks, 2014, 3, 43-49 Published Online December 2014 in SciRes.http://www.scirp.org/journal/etsn.

[16] P. Lakbala, I.D. Kavoos and L. Mahboobeh. 2014. Factors Affecting Electronic Medical Record Acceptance by Specialist Physicians,Lecture Notes on Information Theory Vol. 2, No. 4, December 2014.

[17] M. Aldajan. 2012. Electronic Patient Record Security Policy in Saudi Arabia National Health, PhD thesis, Services, 2012, PhD thesis, De Montfort University, UK.

[18] N. Matar and A. Mohammad. 2014. Evaluating E-Health Services and Patients Requirements in Jordan hospital. International Arab Journal of e-Technology, Vol. 3, No. 4, June 2014.

[19] A. Omotosho and J. Emuoyibofarhe. 2014. A Criticism of the Current Security, Privacy and Accountability Issues in Electronic Health Records, International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 7– No.8, September 2014 – www.ijais.org.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[20] K.B. Rai and A.K. Srivastava. 2014. Security and Privacy Issues in Healthcare Information System, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Web Site: www.ijettcs.org Email: editor@ijettcs.org Volume 3, Issue 6, November-December 2014 ISSN 2278-6856.

[21] A.Y. Hayajaneha and A.A. Zaghloul. 2012. Barriers to the Adoption of Health Information Technology in Arab Countries Hospitals: Practitioners' Perspective. 24th International Conference of the European Federation for Medical Informatics Quality of Life through Quality of Information – J. Mantas et al. (Eds.) MIE 2012 / CD / Short Communications (Poster).
CD / Short Communications (Poster).

[22] D. Gollman. 1999. Computer Security, John Wiley & Sons.

[23] S. Harris. 2003. CISSP All-in-One Exam Guide, 2nd ed., McGraw-Hill OsborneMedia

[24] A. Ferreira, R. Cruz-correia, L. Antunes and D. Chadwick. 2007. Access control: how can it improve patients' healthcare?, Stud Health Techno Inform, (127), p.p. 65-76.

[25] J. Jin, J.G. Ahn, M. Covington and X. Zhang. 2009. Patient-centric Authorization Framework for Sharing Electronic Health Records: in Proceedings of 14th ACM Symposium on Access Control Models Ad Technologies (SACMAT 2009), Stresa, Italy.