AVAILABILITY, ACCESSIBILITY, PRIVACY AND SAFETY ISSUES FACING ELECTRONIC MEDICAL RECORDS

Nisreen Innab

Information SecurityDepartment, College of Computer and Information Security,
Naif Arab University for Security Sciences, Al-Riyadh, Saudi Arabia.

ABSTRACT

Patient information recorded in electronic medical records is the most significant set of information of the healthcare system. It assists healthcare providers to introduce high quality care for patients. The aim of this study identifies the security threats associated with electronic medical records and gives recommendations to keep them more secured. The study applied the qualitative research method through a case study. The study conducted seven interviews with medical staff and information technology technicians. The study results classified the issues that face electronic medical records into four main categories which were availability, accessibility, privacy, and safety of health information.

KEYWORDS

Healthcare information security, electronic medical records security, availability, accessibility, privacy, and safety.

1. INTRODUCTION

Healthcare services are increasingly embracing information technology that allows the automation and digitalisation of health information and manual records. The benefits of this evolution are the convenience and reduction in the cost to healthcare providers, health insurance companies and patients. Medical records at healthcare organisations contain sensitive information about patients. Therefore, these organisations should ensure the security of information, especially because the patients' data is increasingly stored and can be accessed online [1].

Patient information stored in electronic medical records is the most significant set of information of the healthcare system. It assists healthcare providers in offering high quality care for their patients. In hospitals or healthcare centres, electronic medical records contain sensitive information about patients. An electronic medical record contains a patient's demographic data such as the patient's name, gender, contact number and address. Moreover, it contains the diagnosis, procedures, treatments, x-ray images, test results, and any other medical interventions [2].Therefore, it is essential for healthcare providers to have some well-organised form or structure to run electronic medical records data and the patient's information in the health information system. As a result of the sensitivity of patient information, a well-organised structure of sensitive information in health services aims to offer great opportunities of healthcare based on the provision of correct information. Stakeholders could share a patient's electronic

DOI : 10.5121/ijsptm.2018.7101

medical records in order to achieve uniformity of data and simplify the care process. However, without proper security protocols in place, the electronic medical record information may constitute a threat to the patient's privacy and security of information and may be misused by the healthcare provider, insurance companies, or any organisation or party interested in accessing this information for personal use [3].

Healthcare users exhibit an increasing dependency on the available information and specifically, on the information that addresses the valuable assets for healthcare. Thus, the electronic medical records of patients have a critical role in the healthcare system and must be appropriately safeguarded and secured from unauthorised users. Moreover, the communication process among healthcare users regarding patient information must be safe and secured. Healthcare providers should have a security process in place to maintain the confidentiality of a patient's records [4].

Ensuring the security of the health information system maintains the integrity and confidentiality of electronic medical records. When sensitive information is collected and stored in any form or personally identifiable information exists, then a privacy concern appears. Electronic medical records are protected by the health information system security from frauds, intruders, and malware. Protecting patient identifiable information, while sharing this information with different medical practitioners in different departments or places is the main challenge of maintain the privacy of electronic medical records. Privacy of information ensures that only the authorised people get it. This is implemented through many techniques such as data masking, encryption, and authentication [5].

These days, the hacking of electronic medical records by cybercriminals exhibits a gradual rising tendency. Patients' electronic medical records were attacked by hackers. The average sell value differs in some countries from$10 to $1,000 USD of a patient medical record [6, 7].

As shown in table 1in 2015 for each record lost or stolen, the average cost for this break was 363$ in health institutions. Whereas, it was 154$ for the stolen records of other industries [8].

Table 1. Data breach cost per each record in US$ based on industry type.

No.	Industry type	The average cost of data breach per lost or stolen record
1	Health	363
2	Education	300
3	Pharmaceuticals	220
4	Financial	215
5	Communications	179
6	Retail	165
7	Industrial	155
8	Services	137
9	Consumer	136
10	Energy	132
11	Hospitality	129
12	Technology	127
13	Media	126
14	Research	124
15	Transportation	121
16	Public Sector	68

It is greatly important for any nation to develop a general health data centre, which will make it possible to integrate data from various health information systems to be offered for enhanced health services. However, a national health data centre poses a high risk to the privacy of patients and information security. Before integration to a national health data centre, the private and sensitive data of patients reside in a hospital or health centre. Hospitals or health centres are required by law to protect the privacy of data. Nowadays in the case of general health data centres, the circumstances are changed. Therefore, in national health data centres the privacy of patient information may need to be safeguard using appropriate measures [9].

In Jordan, the problem is that electronic medical records have problems in availability, accessibility, privacy, and safety. Therefore, the government should employs an information risk management approach for security purposes in order to prevent the risk of hacking of the electronic medical records. Therefore, this paper aims to identify the security threats that related to availability, accessibility, privacy, and safety and associated with electronic medical records and give recommendations to keep them more secured.The technology in continues development, that leads to continues and variety of difficulties and concerns related to many fields. Our concern in this research is the electronic medical records area

2. LITERATURE REVIEW

2.1 Operational Definitions

A health information system (HIS) is an application that deals with processing data, information, and knowledge involving both computer software and hardware related to healthcare procedures. Moreover, an application is an electronic medical record that includes the clinical decision support, pharmacy, computerised provider order entry, clinical data warehouse, controlled medical vocabulary, order entry, and clinical documentation applications [10].Hakeem program is an electronic medical record applies in Jordan. It depends on a comprehensive open-source health information system. Moreover, it integrates different types of health information systems, including laboratory, pharmacy, administrative, radiology, clinical documentation systems, and computerised physician order entries. The Hakeem program project is constructed on a VistA system. It is used by many countries and has been customised according to their needs. VistAwas deployed and implemented by the US Department of Veterans Affairs [11].

2.2 Health Information System Breach

A research study conducted by the International Business Machines Corporation (IBM) and Ponemon Institute in 2015 revealed that for each incident, on average, more than 18 thousand medical records were breached. In some countries, the average number of breached medical records in a breach incidence was as follows: Arabian countries 29,199; India 28,798; United States 28,070; Germany 24,103; Brazil 22,902; United kingdom 21695; France 20,650; Canada 20,456; Australia 19,788; Japan 19,214: Italy 18,983 [8].For instance in the United States, the total number of electronic medical records breached in 2015 was seven times higher than the total number of electronic medical records breached in 2014. The value of breached records increased from 12.5 Million USD in 2014 to 94 Million USDin 2015[12].

In 2016, hackers attacked the Hollywood Presbyterian Medical Centre. They had shut down the computer system of the centre for about a week for a payoff of 3.7 million USD. It was a

malicious software application called Ransom ware that turned off the system [13].The Hospital Corporation of America (HCA) 2016reported that the electronic medical records were breached as result of staff negligence. The hackers compromised 91,000 electronic medical records for patients. The data affected were social security numbers, dates of birth, and further private information [14].In January 2015, the hackers attacked Premera Blue Cross. The hackers reached the financial and medical data of 11 million patients. Hackers shared financial information, social security numbers, names, medical claims data, addresses, dates of birth [15].

2.3 Previous Studies

Namoglu and Ulgen (2013)conducted a study for Turkish hospitals to uncover the vital components of a 21st century business continuity plan, in the case of which introducing patient privacy auditing standards was achieved on the basis of laws and regulations. The study was applied at a private hospital in Turkey. The researchers conducted interviews with the technical staff in order to determine the technical needs for network security configuration and deployment and with the hospital medical staff in order to perceive the requirements for patient privacy. The results showed that the hospital adopted electronic transactions. These transactions could be accessed by hackers or misused by anyone interested in this information. Therefore, electronic medical records at hospitals must be protected against any attacks or misuse [16].

Alsalamah, Gray, Hiltonc and Alsalamah (2013) investigated patient-centred healthcare support systems to focus on information security requirements. The study results showed that information integrity and confidentiality are the main concerns of the discrete legacy systems in terms of implementing information security. The study used an experimental study, interviews, and observation. The study recognised six requirements needed by a legacy system in order to ensure information security to manage through the circumstances to achieve the balance of security in a system, thus reassuring the provision of patient centred care in current healthcare services. The six requirements of information security were the fine-grained access control; role-based access control; dynamic control; persistent control; circle of trust; and human-level policy awareness [17].

Ozair, Jamshed, Sharma, and Aggarwal (2015) conducted a study entitled ethical issues in electronic health records: a general overview. The study aimed to discuss the various ethical issues arising in the use of the electronic health records and their possible solutions. The study relied on literature to discuss ethical issues in using electronic health records [18].

While our study highlighted specific security issues in electronic medical records, which were availability, accessibility, privacy, and safety. Moreover, the study collected the data from people works in a hospital and deal with electronic medical records. In addition, it focused on electronic medical records (Hakeem program) in Jordan. Finally, it introduced practical solution to these issues.

3. METHODOLOGY

The study used the qualitative research method in order to obtain a comprehensive understanding of the security of the health information system. A case study was conducted to identify the issues and problems, which have not been extensively studied yet. The case study with interviews is the most important technique in order to collect relevant information about specified phenomena. The

study conducted seven interviews with medical members of staff and with an information technology technician (medical record technician, pharmacist, radiologist, medical laboratory technician, physician, supervisor, and information technology technician), who is in direct contact with the Hakeem system at a governmental hospital in order to extract qualitative data from different perspectives so as to know how the security of the health information system was managed. Most participants were male. Their ages ranged between 25 to 40 years. Their education was distributed among three levels diploma, bachelor's and master's degree.

Preplanned questions were prepared prior to conducting the interviews about the security of health information systems. The relevant questions were derived from the literature review and the study goal. Most interview questions were the same. However, the information technology technician was asked some different questions. The questions were reviewed by healthcare researchers and professionals to get feedback and confirm that the study questions make it possible to achieve the study goal. All interviews were conducted at the hospital at a convenient time for the participants. During the interviews, notes were taken by the interviewer. The results of the study interviews were analysed and discussed to reach appropriate solutions to keep the health information system and patients' electronic medical records secure. The interview guide consisted of 15 main questions to find the best way to keep the Hakeem program secure. In addition, some more questions related to the security of electronic medical records were asked to an information technology technician.

4. RESULTS

Information technology has developed very fast. Therefore, electronic health information systems have also developed. However, the study investigated whether electronic health information systems are able to keep sensitive healthcare information secure. As a result, the findings of the participants with different healthcare and information technology technicians in this case study emphasised the significance of electronic records. They considered that electronic medical records are a vital resource of the healthcare system. Most participants mentioned that a secured database is used to store the electronic medical records in governmental hospitals that implement the Hakeem program. Based on the participants' perceptions, the issue with traditional medical records referred to accessing the right information in the right place at the right time. Therefore, providing required medical records or some information takes a long time. The physician mentioned *'in the past, the department of medical records was sometimes late to provide me with traditional medical records that make patients wait more time to get the services'*. With electronic medical records doctors can make a request for any information then they can get it or they can access the required information easily. Any authorised employees can access a specific part of the electronic medical record to add, edit or remove information based on their job. The medical laboratory technician said *'I can access the medical laboratory section and add the laboratory results of patients'*. The system can determine the employee introduced any amendments to an electronic medical record.

Many participants mentioned that the health information system in Jordan (Hakeem program) has attempted to protect and secure electronic medical records from unauthorised users' access. The Hakeem program allows authorised users to access the program after passing the authentication and verification process.
They also said the Hakeem program is a well organised program but still needs to be more secured against unauthorised users and hackers. Changing some information in the electronic

medical record by unauthorised users, hackers or malware can affect patient health negatively. Regarding issues of the electronic medical records, the participants classified the issues that face electronic medical records into four main categories. These categories were availability, accessibility, privacy and safety of health information.Those classification support to decide where the security controls and mechanisms should implemented.

4.1 Availability

The participants mentioned that the Hakeem program was designed to keep electronic medical record secured based on the availability, confidentiality, integrity of information. It is valuable to be sure that the needed health information records are available the authorized people on time. Loss of availability could decrease the service quality, provide inadequate treatment for the patient, financial loss, and some legal issues.

In addition, the system can identify who introduced any amendments to be responsible for that action in the electronic medical record. The information technology technician said *'we can know the person who adds or deletes any information from the medical record based on the username of the person'*.

4.2 Accessibility

Participants mentioned that all new medical records for patients are stored in electronic form. Patients cannot access their electronic medical records. Therefore, if they need a copy of their medical record they should make a request from an authorised person. The medical record technician said *'if patients need a copy of their medical record, they should fill a request'*. Many participants mentioned that every user has limited access to electronic medical records. The access to medical records depends on an employee's task to be performed. This procedure protects electronic medical records from unauthorised employees.

4.3 Privacy

According to the participants, the Hakeem program prevents the information contained in electronic medical records from being accessed by unauthorised employees. Every authorised employee has a username and password. The username consists of the first two letters of the employee’s name and job number. The password can be customised by the employees. The password consists of numbers and letters. The aim of this procedure is to authenticate the authorised person. For example, the employees in medical record departments can access the basic information about the patient. They can add the patient address, telephone number, and nationality of the patient and only preview the electronic medical record, but they cannot access the physician section or add any symptoms of disease or diagnostic.

4.4 Safety of Health Information

The system prompts the employees to change their password regularly. If the employee leaves the computer room without logging out of the system the computer needs a period of time to logout automatically. This period constitutes a risk for sensitive information.

5. DISCUSSION

Electronic medical records are a vital resource of the healthcare system. Therefore, they need to be more secured again unauthorised users and hackers. Privacy rules give patients the right to see information in their medical records, regardless of these being paper or electronic records. Patients have the ability to see or get a copy of their medical record based on the rules of privacy; correct any mistakes in their medical record; choose suitable time to return to the hospital; and make a complain if they do not fully benefit from their rights. These rights are the types of privacy practices given to patients [19]. In addition, protecting the information stored in the electronic medical records of patients consider the rights of the patients. Therefore, the security of electronic medical records requires that health care providers have to set up administrative, physical, and technical protection to maintain patients' electronic medical records safe. A number of safety procedures could be introduced in order to protect electronic medical records. These procedures include access controls like PIN numbers and passwords to help limit records access as well as encrypting techniques [20]. This means that the electronic medical records of patients cannot be read and understood except by healthcare providers who can decrypt this information by using a specific key made available to authorised healthcare providers; an audit trail records who accessed the electronic medical record of a patient, what kind of changes were made and when.

Securely accessing the information within the health system requires three main steps. These steps are the identification of the user that was required to enter a login username; authentication that required users to prove identification via passwords; and authorisation that gives the users the right to access the electronic medical records [17]. Conversely, access control is theoretically an element of the authorisation procedure that verifies if users can access the resources they requested. The healthcare system should include the three steps because the first two steps are essential to the third. Furthermore, several implementations combine the three steps into one access control decision. A health information system that involves the implicit access control policy allowing each employee who is successfully authenticated to access the electronic medical records of patients. This is the hard granularity of the access control policy, in which each employee has the same right to access the Hakeem program. Therefore, the authentication procedure becomes a combined authentication and authorisation mechanism.

The processes of creating an access control system is very complicated and should start with establishing and defining a structured and access control plan in addition to the access control models [21].To deliver the information security requirements of the health information system, an access control plan is needed to determine the rules to be implemented. The naright model of access control should be selected to model the defined rules in the plan. There three common access control models. The Role-Based Access Control that connects the rights to groups of employees according to their job within the healthcare system. The Identity Based Access Control that connects the rights to specific employees depending on their needs. The Mandatory Access Control that describes the fixed rules for all employees of the healthcare organisation [22]. More than one model can be mixed and combined to deal with more varied needs of the healthcare institution. Both access control procedures and authentication and the correct technology can be determined and executed merely after the access control model is chosen. The authentication procedure facilitates the identification and authentication of an employee to the healthcare system (The login username and password), whereas the access control procedure guards against the unauthorised use of the requested resources[17]. Both procedures should achieve in a consistent

and correct manner based on the access control plan and model defined. Providing access control has become more complex. This is required to be implemented cautiously in the healthcare system, thus the access control can be accurately applied and developed without hindering the system's use.

6. RECOMMENDATIONS

1. A health information system should maintain the confidentiality, integrity, availability, and security of its electronic medical records.

2. The Ministry of Health should create laws and legislations or follow international standards to protect sensitive information from unauthorised employees.

3. Implementing the Jordanian health information system (Hakeem program) in all public and private healthcare institutions.

4. Implementing rigorous security access procedures for electronic medical records such as sending the passwords as a message with each access attempt or changing the password compulsory each month.

7. CONCLUSION

One of the significant elements the healthcare system is electronic medical records that needs the proper security system. Nowadays, attackers in rise of targeting the electronic medical records as it worthy for them. Thus, this research investigate some issues and some recommendations to decrease the side impact of those issues. As a result to enhance the security of electronic health information. The study results showed that availability, accessibility, privacy, and safety are the main concerns of implementing secured electronic health medical records. Several mechanisms used to protect the healthcare records to avoid disruption and reduce the risk of information loss. We suggest that international information security standards needs to be followed in The Ministry of Health such as the health insurance portability and accountability act HIPPA. Beside enforce rigorous security access procedures for electronic medical records such as use encrypted passwords. Moreover, as gradually different developing countries implement electronic medical records, we suggest to implement the Jordanian health information system (Hakeem program) in all public and private healthcare institutions.

REFERENCES

[1] Heckenlively, H. (2016). Using Evidence of Industry Standard in Medical Record Breach Cases. Trial Evidence, 24 (1) 5-9.

[2] Khan, S. &Hoque, A. (2015). Towards development of health data warehouse: Bangladesh perspective, in Proc. 2nd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)1–6.

[3] Khan, S. &Hoque, A. (2015). Development of national health data warehouse for data mining, Database Systems Journal, 6(1) 3–13.

[4] Boonstra, A. & Broekhuis, M. (2010). Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions. BMC Health Services Research, 10, 231

[5] Tipton, H. & Krause, M. (2015). Information Security Management Handbook, 6th ed. Northwestern: CRC Press.

[6] McGee, M. (2015). Why hackers are targeting health data. Retrieved from: http://www.databreachtoday.asia/hackers-are-targeting-health-data-a-7024

[7] Humer, C. &Finkle, J. (2014). Your medical record is worth more to hackers than your credit card. Retrieved from: http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

[8] Ponemon Institute (2015). Cost of data breach study: Global analysis.Ponemon Institute, Research Report.

[9] Zhang, Y. &Poon, C. (2008). The development of health care datawarehouses to support data mining. Clinics in Laboratory Medicine, 28(1) 55–71.

[10] Luethi, M.&Knolmayer, G. (2009).Security in health information systems: Anexploratory comparison of U.S. and Swiss hospitals. Hawaii International Conference on System Sciences.

[11] Dua' A. Nassar, Marini Othman and HasnizaYahya (2013). Implementation of an EHR system (Hakeem) in Jordan: challenges and recommendations for governance. HIM-Interchange, 3 (3) 10-12.

[12] Department of Health and Human Services Office for Civil Rights in United States (2016). Breach portal: Notice to the secretary of HHS breach of unsecured protected health information. Retrieved from: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[13] Modern Healthcare (2016). Hospital pays hackers 17,000 to unlock EHRs frozen in 'Ransomware' attack. Retrieved from: http://www.modernhealthcare.com/article/20160217/NEWS/

[14] Health IT Security (2016). 91k patients' data compromised in WA healthcare data breach. Retrieved from: http://healthitsecurity.com/news/91k-patients-data-compromised-in-wa-healthcare-data-breach

[15] Krebs on Security (2015). Premera blue cross breach exposes financial, medical records. Retrieved from: http://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/

[16] Namoglu, N. &Ulgen, Y. (2013). Network security vulnerabilities and personal privacy issues in healthcare information systems: A case study in a private hospital in Turkey. Informatics, Management and Technology in Healthcare, 9, 126-128.

[17] Alsalamah, S., Alex, W., Hilton, J., Alsalamah, H. (2013). Information security requirements in patient-centred healthcare support systems. MEDINFO, 9, 812-816.

[18] Ozair F, Jamshed N, Sharma A. & Aggarwal P. (2015). Ethical issues in electronic health records: A general overview. Perspective Clinical Research, 6, 73-76.

[19] Alanazi, H., Zaidan, A., Zaidan, B., Mat Kiah, M. & Al-Bakri, S. (2014). Meeting the Security Requirements of Electronic Medical Records in the ERA of High-Speed Computing. Journal of Medical Systems, 39,165-177.

[20] Monterrubio, S., Solis, J., Borja, R. (2015). EMRlog Method for Computer Security for Electronic Medical Records with Logic and Data Mining. BioMedResearchInternational, 15, 12 pages.

[21] Hu, V., Ferraiolo, D., & Kuhn, D. (2006). Assessment of Access Control Systems. National Institute of Standards and Technology, U.S. Department of Commerce, Interagency Report 7316.

[22] Abel, N., John, P., Kathryn, L. et al. (2015). Design and implementation of a privacy preserving electronic health record linkage tool in Chicago. Journal of the American Medical Informatics Association, 22(5), 1–9.

[23] Sher, M., Talley, c., Cheng, T. &Kuo. (2017). How can hospitals better protect the privacy of electronic medical records? Perspectives from staff members of health information management. Health Information Management Journal, 46(2), 87-95.

AUTHOR

Dr. NisreenInnab got her Ph.D. in 2008 in Computer Information System, she was employed as full time lecturer, Assistant Professor and MIS department Chairperson at University of Business and Technology in Saudi Arabia, Jeddah from 2007 to 2010. Then she was worked from May 2011 to August 2014 as a honorary researcher and master thesis examiner in the school of science and technology at University of New England, Armidale, Australia. Finally, from September / 2016 till now she works in the department of information security at Naif Arab University for Security Sciences, Riyadh, Saudi Arabia. She published nine papers in international journals and conferences. Her current research interests are: information security, data mining, machine learning, modeling and simulation, ontology, modeling diagrams.