MANAGING THE INFORMATION SECURITY ISSUES OF ELECTRONIC MEDICAL RECORDS

Nisreen Innab

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

ABSTRACT

All healthcare providers should have enough knowledge and sufficient information to understand the potential risk, which can lead to a breach in the Jordanian health information system (Hakeem program). This study aims to emphasise the importance of sharing sensitive health information among healthcare providers, create laws and regulations to keep the electronic medical records secure, and increase the awareness about health information security among healthcare providers. The study conducted seven interviews with medical staff and an information technology technician. The study results showed that sharing sensitive information in a secure environment, creating laws and regulations, and increasing the awareness about health information security render the electronic medical records of patients more secure and safe.

KEYWORDS

Electronic Medical Records Security, Health Records, Data Breach, Hakeem Program.

1. INTRODUCTION

There is much essential information required to be shared among healthcare providers. This information includes hospitalisation, prescription drugs, ambulatory patient services, emergency services, laboratory services, mental health and substance use disorder services, including behavioural health treatment, maternity and new-born care, treatment and rehabilitative devices and services, paediatric services, preventive and wellness services, and chronic disease management. It is hard to find all of this complicated information about patients' services in an individual healthcare organisation. Therefore, it should be secure sharing and conveying the effective communication of electronic medical records among multidisciplinary providers, divisions, and other healthcare organisations [1]. Sharing information between divisions and healthcare organisations is a challenge faced by healthcare providers. Risk in the healthcare system of patients' electronic medical records security can be more complex when care includes healthcare providers, who have autonomous information technology network security frameworks in place with potential weaknesses.

The privacy of electronic medical records is separated into two groups: issues regarding data security and issues regarding patient's information confidentiality. Legislations, which are planned towards maintaining the confidentiality of patients through leading the actions in which hospitals are able to reveal information can also deliver incentives for the security of patient data [2]. Privacy laws raise the network benefits or the network costs from the adoption of electronic medical records. The laws of privacy can increase the benefits of the network as they enhance

patient fulfilment by reassuring for the patients that the way of treating and transmitting their medical records among health providers is secured and confidential. A survey shows that 8% of patients believed they sensed that their medical information in a clinic or hospital had been unacceptably revealed [3]. Disclosed personal medical information has led to appealing in privacy-protecting behaviours for the medical information (avoiding embarrassing medical tests) for 13% of patients [2]. These worries are important for patients' information when exchanged electronically. In order to increase the willingness of these patients to make them share their health information in an honest way and undergo testing or risk factors, a privacy law is required. As a result, the health providers, while using electronic medical records to exchange the health information would be beneficial to improve the quality of healthcare.

The security threats can be converted into healthcare assets because of lack of knowledge, unawareness about the fundamentals of information security, that result in a variety of potential risk factors to the security of any organisation. In addition, hospital staff do not have enough knowledge about the standards and policies or they are most likely not correctly trained in information security in general, access control list, and physical security. There is a lack of basic training and procedures for guidance to increase the information technology awareness of hospital staff. This implies that, the awareness of a strategy needs to be projected with a view to ensure responsibility [4]. All healthcare providers should have enough knowledge and sufficient information security education in order to understand the potential risk, which exists inside and outside the healthcare organisation system. The education could be around issues, such as being able to identify phishing attempts. Moreover, it can also focus on the importance of right practices, such as not leaving laptops without attendance or writing a password on a notebook. Hospital staff and information technology should also entail security of information, the way in which transactions take place and of the resources used [5]. Figure 1 showed the number and percentage of health record breached between 2012 and 2015 in USA. As presented %81 dramatic increase in breaching health records in 2015, whereas, in 2014, 2013, and 2012 the percentage of electronic medical records breached were %11, %6, and %2 respectively [6]. Therefore, the users of electronic health records need to share these sensitive information in secure way and obtain more awareness. Indeed, rigid laws and regulations required to protect these records.

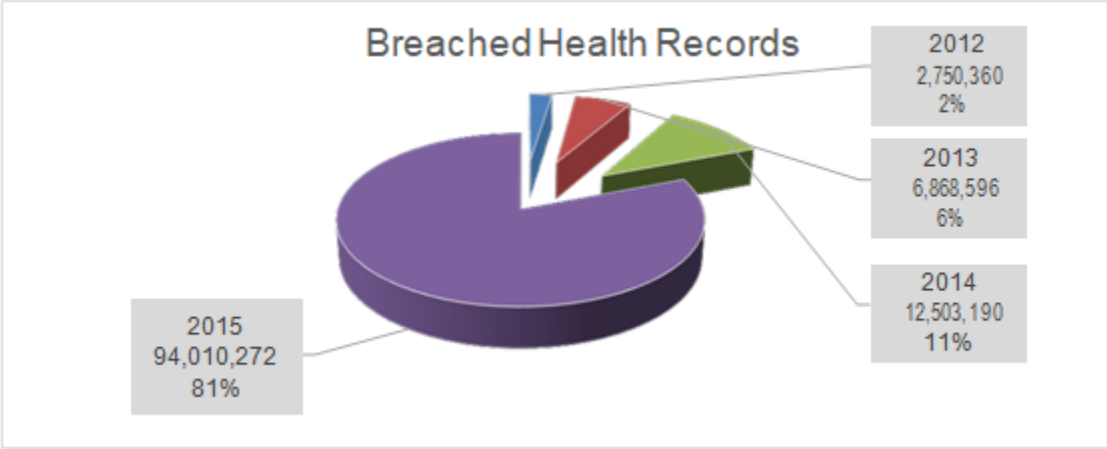

Figure 1: The number and percentage of breached health records between 2012 and 2015

Many factors need to be considered in providing and transforming information in electronic health medical records. Some of those factors are sharing sensitive information, laws and regulations of health care, and awareness of health information security. This paper provides a discussion of those factors and its implications on health electronic records. Moreover, it deliberates some of the challenges of those three factors. Then it provides some recommendations to tackle the impacts of the challenges.

2. LITERATURE REVIEW

2.1 HAKEEM PROGRAM

The health sector in the Hashemite Kingdom of Jordan was computerised by the Health Computing Company. It is a non-profit company. The Hakeem program was launched in 2009 and it was applied in different public hospitals and health centres. The Hakeem program aims to improve medical services, increase the effectiveness of medical management and reach the best international standards, as well as improve health economy. The Hakeem program relies on a developed VistA system, used in the hospitals and clinics of the US Department of Veterans Affairs [7].

VistA is an open source system, which provides the ability to access and update the software code. VistA is designed and developed specifically for medical purposes. The Hakeem program has many benefits. First, it creates and maintains electronic medical records for patients that leads to faster and safer treatment, it also improves the level of health care services. Second, it reduces operational costs in health institutions through the optimal use of resources by storing electronic medical records. Finally, the program contributes to the creation of a comprehensive database of patient data to support research and scientific development [8].

2.2 HEALTH ELECTRONIC RECORDS BREACHES

Individual health medical records contain information that could be obtained by individuals or organisations based on the rules of an agreement of confidentiality, which cannot be freely obtained through other public means. When this data from the medical records is exposed or lost, then this is referred to as a of health data [9]. According to the time and the place of the cause and protection of the breach of data, the costs may vary. 154 USD was the average cost of the data breach of each stolen or lost record, where it was 363 USD for health breach [10]. According to the 2015 Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, which covered 90 healthcare organisations in the USA, more than 90% of all healthcare service providers experienced a data breach, and 40% had more than five data breaches over the past two years. In 90 healthcare organisations in the USA, data breach was experienced by more than 90% of healthcare service providers, and over the past two years 40% had more than five data breaches [11]. Breaches of Protected health information drastically impact on the goodwill of a healthcare organisation. In a research report it is shown that, people are withholding their health information from healthcare providers because they are concerned that there could be a confidentiality breach of their records. An unwillingness to fully disclose information could delay the diagnosis of a communicable disease. This is not only a potential issue for the treatment of a specific patient; there are potential public health implications. People are concerned that there could be a confidentiality breach of their records, so they are with holding their health information from

healthcare providers based on a research report. The goodwill of a healthcare organisation is significantly affected by breaches of protected health information [8].

2.3 PREVIOUS STUDIES

Khan and Hoque (2016) conducted a study about digital health data and provided a state of the art review of the threats of security in health information systems. Based on the study results, the servers of healthcare organisation data are the leading target of hackers due to their

monetary value. The study also found that nowadays, healthcare data breaches are 1.25 times greater compared to five years ago. It is recommended that healthcare providers should implement rigorous procedures in order to minimise and reduce the risk of attacks and maintain the privacy of electronic medical records [12].

Orel and Bernik (2013) conducted a study focused on the implementation of healthcare information security. The researchers evaluated the common approaches widely used in the security of systems in healthcare, along with the level of awareness, acceptance and confidence of significant standardisation. They mentioned that patients' information in electronic medical records is sensitive, and thus putting proper techniques and procedures as well as modern technology in place to secure healthcare information is of vital significance. Computers, tablets, and mobiles are becoming the top priorities in information security planning with healthcare organisations being no exception. There is less application in healthcare without having a need for a mobile functionality, which faces healthcare providers with the challenge of rendering patient information more secure. This is also true in outpatient clinics, emergency treatments, homecare and rehabilitation just to mention a few areas outside healthcare organisations controlled environments. However, traditional unsecured communication between healthcare organisations and departments is still routinely used for communicating sensitive healthcare information. The security awareness level with healthcare professionals, users, and patients is not high enough such that potential risks and threats could be addressed and the vital information security management is therefore weak. The researchers recommend using standards, such as the ISO/IEC 27799 information security guidelines in health and consider these standards in legislation [13].

Luethiand Knolmayer (2009) examined the security of health information systems in U.S. and Swiss hospitals. Their empirical research showed that the security of health information systems lacks some controls. In addition, the size and information technology flow as well as the specific regulations affecting the security of health information systems. Moreover, usage varied application systems and various patterns of medical staff exacerbate security efforts. Technical security controls of health information have become an important fragment of the lifecycle of the health system. Nevertheless, they still want further authentication controls and progressive security [14].

3. METHODOLOGY

The study used the qualitative research method in order to gain a comprehensive understanding about the security of the health information system. This case study was applied in a public hospital in Amman. The study applied the case study method in order to gather deep information from different perspectives about the security system in the Hakeem program. The study conducted seven interviews with medical staff and one information technology technician at a

public hospital in March 2017. The medical staff who participated in this study included a medical record technician, pharmacist, radiologist, medical laboratory technician, physician, and supervisor. These participants were chosen because they were in direct contact with the Hakeem program. Open-ended questions were prepared with reference to the security of patients' information in the Hakeem program. The questions were directed based on the study goal. The interviewee questions were sent to healthcare managers and Ph.D. holders in health services management to make the questions more convenient to achieve the study goal. The questions for medical staff were the same. Some additional questions were asked to the information technology technician. The interviews were conducted in the workplace at a convenient time for the participants. The participants announced their verbal consents for willingness to participate. Brief information was given to participants. A semi-structured interviews prepared for them. Informal conversational style with some prompt questions was used as an approach for each interviewee. The length of interviews time were varied from 50 to 60 minutes. Notes were documented directly during each interview. The first step of the interview processes was greeting the participant. Then collecting demographic information about the participant and brief background. Next, the participant started answering the study questions. After that a conclusion was drawn. Finally acknowledging the participant. The thematic analysis approach was used in order to analyse the data. The data were distributed among three main themes. These themes were sharing sensitive information; laws and regulations of health care; and awareness of health information security.

4. RESULTS

4.1 SHARING SENSITIVE INFORMATION

Most participants declared that the health information system (Hakeem program) in Jordan, shared electronic medical records among hospitals that implement the Hakeem program. The Hakeem program has a centralized database system to store patients' sensitive information in a secure manner. The medical record technician said 'we store electronic medical records on a centralized database'. In addition, there is back up copy for all electronic medical records. The healthcare providers in other hospitals can access the patient's information based on their authority to understand the patient situation. The problem is that if patients moved to get treatment in a hospital that does not implement the Hakeem program, the healthcare provider who works in the latter hospital cannot access the electronic medical record in the former hospital that uses the Hakeem program. The information technology technician asserted, *'there is no connection between Hakeem program in public hospitals and electronic medical records in private hospitals'*.

Participants emphasise that when a hospital would like to transfer a patient to another hospital due to the occurrence of a critical situation, the hospital follows a traditional method. This is considered unsafe for patient information. This means that the hospital should provide the patient with a referral letter to be moved to another hospital for further treatment. The referral letter has basic and critical information about the patient status. This method of handling critical information is considered unsafe for the patient because any employee in the referral hospital could receive or read the referral letter.

Most participants mentioned that the Jordanian government has a plan to join all public hospitals with the Hakeem program. The information technology technician said *'we implement the*

Hakeem program in most public hospitals and we are going to connect the rest of them with the Hakeem program soon'. It also needs more attention to connect the Hakeem program with private sector hospitals. This procedure reduces the paperwork required to transfer information and render the treatment process faster. However, the extensive use of the Hakeem program could make it easier for hackers to access the program. Therefore, rigorous procedures should be implemented to keep the Hakeem program safe.

4.2 LAWS AND REGULATIONS OF HEALTHCARE

Most participants declared that the ministry of health in Jordan has many laws or regulations to maintain and improve healthcare services in Jordan. These laws or regulations neither concentrate on the protection of sensitive information or electronic medical records nor focus on security requirements. The physician said, *'there is no any laws or regulations focused on the security of sensitive information or electronic medical records'*.

Many of the participants mentioned that the implementation of the Hakeem program in public hospitals required the ministry of health to create laws, legislations and standards to protect the electronic health records. These laws, legislation, and standards are essential to keep the relationship between patients and healthcare providers secure. Moreover, every employee in a hospital should know the laws, legislation, and standards that concern on protect patient information.

4.3 AWARENESS OF HEALTH INFORMATION SECURITY

Participants declared that employees in public hospitals do not have enough awareness about the sensitivity of the information available in electronic medical records. There are no lectures or seminars held to provide employees with basic knowledge about the sensitivity and security of electronic medical records. The radiologist said *'the hospital did not hold any lectures to increase the awareness about the sensitivity of the health information of patients'*.

Many participants mentioned that the hospitals that implement the Hakeem program should give more attention to information security in the healthcare system. They should create instructions regarding information security. In addition, it is equally important to initiate training programs to provide employees with more information about the importance of keeping electronic health records secure. Lack of education in the field of health in relation to information security leads to careless employees and risks that can affect sensitive information in the healthcare sector. Furthermore, employees should be aware of the importance of antivirus applications on the computer and they should not access any unverified web sites or open any strange links because that could allow hackers to breach the Hakeem program.

5. DISCUSSION

Hospitals, which are not connected yet with the Hakeem program, can use email messages for communication. They should identify the patient by using the medical record number of patient in the body of the email message. Hospitals should prohibit the use information that leads to the easy identification of patients such as full name, email address, telephone number or full face photograph. If this information has to be included, it is necessary to be attached in an email message with a password encrypted file. Each password should be complicated and must not be

communicated via email. It has to be sent to the intended person in the intended hospital via telephone [15]. This procedure must be used for all patients especially for those affected by highly sensitive diseases, such as substance abuse treatment, mental health problems, or the Human Immunodeficiency Virus (HIV). Hospital employees should always use trusted, secured and formal emails accounts, such as hospitalname@moh.gov.jo when they intend to received or send patients' information to other hospitals not connected to the Hakeem program. Patients' information should be sent by email after the recipient's address has been entered correctly and carefully verified. Patient information must never be sent to personal email accounts. The end of each email should have a privacy statement referring to the privacy of information and prohibiting the misuse of patient patient's information

Sensitive health information leads to vast debates as to whether it should be considered as a separate category form other different health information categories. Many believe that sensitivity is subjective. Based on the characteristics of a person's life circumstances, health situation and feelings, and political and cultural standards, sensitivity may differ. Generally if sensitive health data is exposed, this can lead to remarkably great risks such as social disgrace, physical harm, and discrimination. Also the risk could affect the person's family such as disclosure for genetic information. The classification of health information, which is considered sensitive, consists of genetics, domestic violence, reproductive care (including abortion), mental health, substance abuse, sexually transmitted disease information, and personal information [16].

The ministry of health in Jordan should create laws and regulations to protect electronic medical records. These laws and regulations should provide a powerful comprehensive solution to address electronic health record data integrity and security. Laws and regulations in the health system should address privacy protection, ethical and legal concerns, regulations concerning the access and disclosure of electronic medical records [17].

The value of electronic medical records to a cybercriminal is enhanced by the fact that hospital employees are generally busy with heavy work duties. That means they have to accomplish many important jobs related to patients' lives. This makes the employees pay less attention to the electronic medical records of patients because they have a lack of security awareness. Cybercriminals can utilise any mistakes of employees to breach electronic medical records, such as leaving the computer room for a long time without turning off the computer or an employee could click on a phishing link which could lead to the loss of thousands of electronic patient medical records. Becoming security aware is much needed in hospitals under such a severe and relentless threat. Authorised employees need to be more cautious as part of their remit [18].

Information technology employees are also on the front line in terms of electronic medical records security. They have job duties to ensure that system and hospital employees are security aware. Their job duties should also include adding extensions to cover associated hospitals and insurance companies outside the hospital environment; covering situations that patients electronic medical records be digitally communicated to a third party in a secure manner; extending compliance requirements such that information technology employees and hospital employees involved in security and compliance, need to have a strategy to protect the electronic medical records; requiring information technology employees to look after immediate electronic medical records protection concerns as well as extended touch points into the health system through associated bodies; and ensuring that security policies are adopted in an effective and efficient manner. Information technology employees can utilise their training and security awareness

knowledge to ensure that electronic medical records are at the forefront of the security mitigation techniques.

6. RECOMMENDATIONS

1. Some guidelines need to be applied to the dissemination of sensitive health information in order to protect sensitive health information such as Fair Information Practices (FIPs).
2. Each health service provider need to create dedicated policy of sharing sensitive patients' information.
3. Patients should recognize the rules and the policy of sharing sensitive information to ensure for them that their information will kept secured as they expected.
4. Healthcare institutions should implement education or training programs for their employees with an emphasis on the importance of keeping electronic medical records secure.
5. Regular training programs should introduce for information technology technicians to keep them exposed to new programs, systems, and technology that focus on information security.
6. Governments required to state rules for keeping health medical records secure.
7. The responsibility of each health provider is to encourage his staff and users to follow security medical records rules.
8. Hakeem program required to be implemented in all Jordan health institutions because it has the capability to save the sensitive information of patients in a centralised database system in a secure manner.

7. CONCLUSION

Health medical records are used to increase the quality of the health care service. However, along with the use of electronic records, some of the concerns refer to preserving the security of the health information. It is essential to have some ways to ensure that the dissemination of sensitive information is protected, health care laws and regulations are implemented, and the awareness of health information security is broadened. As a result, it is necessary for the individual to know that when they seek health care treatment, their health information is secured.

It is the responsibility of the health care provider to protect the sensitive information of patient while it's transmitted and shared among the health employees. Because most of the patients keen to keep their sensitive medical history private. It is unsecure to use the traditional method of transferring the health information between the staff of the same health institution, neither between different health institutions in case the patient situation need to move from one to another. Consequently it is recommended to use in Jordan for all health institutions Hakeem program which is automated electronic health record solution. Where all the health staff are able to share the health information in easy and fast way through electronic access if they authorised to do so. Strict laws and regulations should be implemented with implementing and using Hakeem program to keep it safe from hackers. Furthermore, training programs should introduced to health employees who may use Hakeem program to increase their awareness of the significant of the security of electronic medical records.

REFERENCES

[1] Key, D. & Ferneini, E., (2015) "Focusing on Patient Safety: the Challenge of Securely SharingElectronic Medical Records in Complex Care Continuums", ConnecticutMedicine, Vol. 79, No. 8, pp 481- 485.

[2] Miller, A & Tucker, (2009) "Privacy protection and technology diffusion: the case of electronic medical records", Management Science, Vol. 55, No. 7. pp 1077–1093.

[3] Kazley, A. & Ozcan, Y., (2007) "Organizational and environmental determinants of hospital EMR adoption: A national study", J. Medical Systems, Vol. 31, No. 5, pp 375–384.

[4] Marvin (2017) "Health Information Technology: Integration, Patient Empowerment, and Security",Am J Health-Syst Pharm, Vol. 74 No. 2, Pp 36-38.

[5] Humaidi, N. & Balakrishnan, V., (2015) "The moderating effect of working experience on health information system security policies compliance behavior", Malaysian Journal of Computer Science, Vol.28, No. 2, pp 70-92.

[6] Khan, S. & Hoque, S., (2016) "Digital health data: a comprehensive review of privacy and security risks and some recommendations", Computer Science Journal of Moldova, Vol. 24, No. 2, pp 273-292.6

[7] Dua', A., Marini, O & Hasniza, Y., (2013) "Implementation of an EHR system (Hakeem) in Jordan: challenges and recommendations for governance", HIM-Interchange, Vol. 3, No. 3, pp 10-12.

[8] Electronic Health Solutions, (2017) "Benefits of Hakeem Program", Retrieved from http://ehs.com.jo/hakeem-program/benefits-hakeem

[9] Howard, P.,(2014) "Data Breaches in Europe: An Analysis of Reported Breaches of Compromised Personal Records in Europe", Center for Media, Data and Society Central European University. Retrieved from: http://cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/article/663/databreachesineurope.pdf

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

[11] Ponemon Institute, (2015) "Fifth annual benchmark study on privacy & security of healthcare data", Ponemon Institute, Research Report.

[12] Khan, S. & Hoque, A., (2015) "Development of nationalhealth data warehouse for data mining",Database Systems Journal, Vol. 6, No. 1, pp 3–13.

[13] Orel, A. & Bernik, I., (2013) "Implementing healthcare information security: standards can help",Implementing Healthcare Information Security: Standards Can Help, Vol. 186, pp 195-199.

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

[15] Vest, J. & Kash, B., (2016) "Differing strategies to meet information-sharing needs: Publicly supported community health information exchanges versus health systems' enterprise health information exchanges", The Milbank Quarterly, Vol. 94, No. 1, pp 77-108.

[16] Bansal, G., Zahedi, F., & Gefen, D., (2010) "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online", Decision Support Systems, Vol 49, No 2, pp 138-150.

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

[18] Aydın O. & Chouseinoglou, O., (2013). "Fuzzy assessment of health information system users' security awareness", Journal of Medical Systems, Vol. 37, No. 6, pp 84-99.

AUTHOR

Dr. Nisreen Innab 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.