Egyptian Informatics Journal 22 (2021) 177–183

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Review

# Security and privacy of electronic health records: Concerns and challenges

Ismail Keshta [a,*], Ammar Odeh [b]

[a] Computer Science and Information Systems Department, College of Applied Sciences, AlMaarefa University, Riyadh, Saudi Arabia
[b] Computer Science Department, Princess Sumaya University for Technology, Amman, Jordan

ARTICLE INFO

*Article history:*
Received 8 August 2019
Revised 9 July 2020
Accepted 24 July 2020
Available online 4 August 2020

*Keywords:*
Electronic health records
Privacy
Confidentiality
Security

ABSTRACT

Electronic Medical Records (EMRs) can provide many benefits to physicians, patients and healthcare services if they are adopted by healthcare organizations. But concerns about privacy and security that relate to patient information can cause there to be relatively low EMR adoption by a number of health institutions. Safeguarding a huge quantity of health data that is sensitive at separate locations in different forms is one of the big challenges of EMR. A review is presented in this paper to identify the health organizations' privacy and security concerns and to examine solutions that could address the various concerns that have been identified. It shows the IT security incidents that have taken place in healthcare settings. The review will enable researchers to understand these security and privacy concerns and solutions that are available.


**Contents**

1. Introduction . . . 177
2. Concerns on privacy and security of electronic health records . . . 179
3. Security and privacy features of current EHR systems . . . 180
4. Information technology security incidents in health care settings . . . 182
5. Conclusion and future work . . . 182
Declaration of Competing Interest . . . 182
Acknowledgements . . . 182
References . . . 182

## 1. Introduction

An electronic health record is defined as an electronic version of a medical history of the patient as kept by the health care provider for some time period and it is inclusive of all the vital administrative clinical data that are in line to the care given to an individual by a particular provider such as demographics, progress reports, problems, medications, important signs, medical history, immunization reports, laboratory data and radiology reports [15]. Use of paper as a means of recording health data in most healthcare facilities and organizations has led to an extensive paper trail and most organizations have developed interests in shifting from paper-based health records to electronic health records. Carey et al. [14] explains that integrated health records are much effective and have more benefits such as lowering costs, improving health care quality, promoting evidence-based medicine usage and helping in record keeping and ensures mobility of the records. To remain effective, electronic health record system must satisfy

* Corresponding author at: Computer Science and Information Systems Department, AlMaarefa University, Riyadh, Saudi Arabia.
*E-mail addresses:* imohamed@mcst.edu.sa (I. Keshta), a.odeh@psut.edu.jo (A. Odeh).
Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.eij.2020.07.003
1110-8665/

some requirements such as achieving complete data, resilience to failure, be highly available and be consistent to security policies [4]. However, there are a number of factors that have hindered the application of electronic health records. They include funding technology, some aspects of the organization and attitude.

A good number of governments have shown interest in using integrated electronic health records due to the expected benefits; for instance the government of USA in 2004 made a decision that most Americans were to be connected to an electronic health records system by the year 2014 [31]. Later on, the American Recovery and Reinvestment Act of 2009 included setting aside a total of $19000 million to be used in digitalizing health care records in the United States [12]. Likewise the European Union countries had planned to ensure that they had a common health system by the year 2015 according to the High Level eHealth conference that was held in 2010. The objective of the European Union countries to perform sharing of patients electronic health records data in realizing quality and efficient health services [12]. However, very little has been done in developing policies to address the privacy concerns that were raised by shifting from the use of paper in storing health records to an electronic health record that could also be integrated [55]. Moreover, the growth on Information and Communication Technologies has resulted into a scenario whereby the health data of patients are affecting the security and privacy threats. Presently, there are a lot of concerns regarding privacy and security of protected health data and these concerns are the biggest barriers in implementing electronic health records; and hence the need for health organizations to find out strategies that can help them secure electronic health records [46].

Electronic Health Records are also referred to as electronic medical record (EMR) and their use is gaining popularity under the topic of e-health [1]. Electronic medical records contains patients' health-related data and is classified as a major factor in the application of e-health. Electronic medical record is made up of legal records that are composed at the hospital environments. These data are then used as the main source of data for electronic health record [1]. Even though hospitals use electronic medical records system in their day to day services, the experience of the healthcare professionals makes them not fully trust the system. Albahri [3] explains that the terminology e-health featured in the early 21st century and it involves utilizing modern methods of information and communication to convey medical services in the health care sector. Effectively managing an Electronic-health requires multidisciplinary team including telecommunication, instrumentation, computer science to enable exchange of medical data across wider geographic regions [39]. The use of e-health enables the users to have a wider thinking and allows health care providers to network effectively [35]. Improving the healthcare has benefits such as improving the efficiency of healthcare operations and improves the quality of health care services offered to patients.

'Electronic medical record' and 'electronic health record' are separate terms that contains patients' health related information and is the basis of e-health application [49]. These records are so useful to all health professionals [49]. Electronic health records allows the medical information shared amongst stakeholders very easily and the patient information be accessed and updated as a patient undergoes treatment. Alsalem et al. [5] explains that health information technology can greatly improve the efficiency, patient safety and healthcare outcomes while reducing the cost. EHRs could benefits such as saving cost by digitizing the data system and having a central place for providing medical data [5]. However, for a very long time, the health statistics has mainly been paper-based records. However, there have been tremendous changes in the last three decades with the increasing application of health information technology.

Literature has talked about security issues that come from trends in information and technology for instance keeping health records on distant serves operated by third-party cloud service providers [1,23]. Health Information Technology refers to all the information technology systems used in storing, accessing, processing, sharing and transmitting health information or support health care delivery and healthcare system management. The information that the Health Information Technology contains are very sensitive and the information includes data related to patient's tests, diagnoses, treatment together with information on the patients' medical history [16,28,29]. It is therefore very important that these information is secured so that it is not manipulated enabling patients to continue sharing information pertaining to their health and work considering the moral and legal responsibilities. However, ensuring that the health records are secure is negatively affected by the dynamic nature of the Health Information Technology environment [57].

The common issues that needs to be addressed in electronic medical record system are privacy, security and confidentiality [2]. Although security and privacy are strongly related, they are in real sense different. Privacy refers to the right that someone has to determine for themselves when, how and the level at which accessing personal information is transferred or shared by others while on the other hand, security is defined as the level at which accessing someone's personal information is restricted and allowed for those authorized only [26,57]. Transferring or sharing sensitive health data when not authority can lead to data breach. Privacy can as well be breached in many situations through unpreventable systemic identification that occurs in the entire electronic health infrastructure and by central technologies and parties that look at the actions of healthcare workers and patients [57]. However, in some cases the government, employers, pharmaceutical companies, researchers and laboratories could have valid reasons to access the health records of patients so that to get some data and in the process, the health care provider could abuse the health records access either accidentally or intentionally [17].

Dehling and Sunyaev [21] also suggested that the three basic information technology security requirements are confidentiality, integrity and availability. Confidentiality can be defined as restricting information to persons that are not authorized to access data during either storage, transmitting or when they are being treated. Confidentiality can be achieved through technological means such as data encryption or through controlling accessing the systems. Confidentiality is also achieved through working on moral dispositions such as professional silence [13]. However, it was realized by [21] that although encryption is mostly used for health data that are sent across exposed networks, it is less applied to data that is stored in mobile devices and other storage media [21]. The need for confidentiality is a response to privacy concerns that are also very important in the health care sector due to the very sensitive data regarding patients and clients that they carry. Dehling and Sunyaev [21] mentioned that confidentiality ensures that the information remains protected from unauthorized deletion or modification and undesired modification by authorized users. On the other hand, availability ensures that a system can be accessed and is fully operating at any moment that an authorized person is in need of using them. Availability means a number of aspects from scalability to resilience and to recoverability of data in case the data is lost for any reason [21].

Physicians are normally very concerned that an unauthorized person could access the information of patients that are stored in the electronic medical records system and misuse the information hence leading to a legal complications following a breach in the confidentiality of the patients' records [49]. Wikina [62] suggested that physicians are very keen on the security and confidentiality concerns more than the patients themselves. The majority of doc-

tors who use electronic medical records prefer paper records more than electronic medical records because they believe that paper records are much more secure and confidential. This is an indication that the issue of privacy and security on EMR is taken very seriously. If the patients are not assured privacy, they could decide to withhold the information to prevent inappropriate use [34].

Many countries are therefore in the process of reforming their health care services through application of Information Technology [42]. The use of IT has helped individuals improve their care experience, improve health of population, and reduces health care cost [56]. The present developments in Information Technology has resulted to a digitalized health records and therefore creating a new or improved ways to successfully do collection, processing, storing, consulting, and sharing of health information. Digitized health information are more portable and can be shared among health care organizations, are much more available to the public health administrators conducting health surveys making policies and is also available to patients. So far, most literature have suggested positive effects of a digitalized system on healthcare outcomes [42]. However, these digitalized health information expose health records to security breaches related to information technology [43]. Potential users of health Information Technology are much concerned with the information technology related security and privacy which negatively affects the trust of electronic health records [43]. This reduction in trust from health care professionals and patients may not fully welcome the use of electronic health records and therefore threatening information technology importance [43]. This can later lead to ineffective healthcare delivery [41] as well as ineffective public health monitoring or health research [59].

It has been suggested by Liu, Musen & Chou [47] that it is important that the methods of providing cyber-security that are associated with electronic health record needs to be well understood prior to their implementation. The information that is stored within the EHR is very sensitive and therefore so many security features were initiated by the Health Information Technology for Economic and Clinical Health Act and the Health Insurance Portability and Accountability (HIPAA) Act [24]. HIPAA outlines three pillars that it uses in ensuring that the protected health information remains secure by applying administrative safeguards, physical safeguards, and technical safeguards [36]. The three pillars are also called the healthcare security safeguard themes and they range from techniques protecting computers' location to the application of firewall software in protecting health information.

It is important to note here that EHR is being increasingly used in a number of developing nations as it not only improves healthcare quality but is cost-effective as well. Technologies such as this can create hazards, therefore, it is a real challenge to safeguard the safety of the information that exists in the system. Security breaches have recently raised concerns about this system. Although it is becoming ever more useful and there is growing enthusiasm for its adoption, little attention has been given to the security and privacy issues that could arise as a result. Therefore, the authors have undertaken in-depth analysis of all the relevant issues associated with privacy and security features of EHR system as reported in the public scholarly literature using a comparative framework developed from ISO 27799 standard. Literature has identified that EHR solutions acquired from various vendors usually comes with an already set of security and privacy capabilities and the present question could only be answered by analysing the specific real solutions that are used as EHRs. Moreover, the authors strongly believe that if the privacy and security proposals found in the published scholarly literature are highlighted and analysed, they could subsequently be applied as proxy for what might be the real EHR privacy and security proposals. This research could as well provide useful information for the stakeholders in the healthcare system as well as other agencies on the need to implement, select, develop and use some specific Electronic Health Records that enhance privacy and security of the patients involved. The present paper is equally purposed for custodians who have the responsibility of overseeing the security and privacy of information systems within the healthcare sector. The paper can also be used by other scholars as a reference point on how security and privacy of the patients can be enhanced in the electronic health record systems.

The rest of the paper will be organized as follows. Section 2 highlights concerns on privacy and security of electronic health records. Section 3 presents security and privacy features of current EHR Systems. Section 4 illustrates information technology security incidents in health care settings. Then, finally, Section 5 will discuss both the paper's conclusion and any future research directions.

## 2. Concerns on privacy and security of electronic health records

Many surveys have reported many concerns regarding the privacy of health information. Win [63] suggested that close to two thirds of clients paid attention to privacy of their personal health records and only 39% of the respondents felt that their health data were safe and secure. In some cases, the respondents the respondents neither worried about the security of their data nor had faith that their data would be safe [45]. Perera et al. [52] carried out a study in which half the respondents explained that they were worried about the security of their data because it had to travel through the internet. Close to half of the research participants in a study conducted by Ancker et al. [7] believed that exchanging their health information could worsen their health information privacy. Meanwhile, a number of studies that were aimed at investigating individual concerns for information privacy realized that they were essential in the realization of successful electronic health records technologies.

Privacy and security challenges of the internet of things start from the given characteristic of the internet of things networks, which make them unique in their own ways. Such characteristics are heterogeneity, uncontrolled environment, constrained resources, and the greater need for scalability. Even the smallest processor platforms presently have a very nice crypto engine and sufficient program memory for implementing relevant security functions. Lafky & Horan [45] proposes that security requirements for the Internet of Things systems, depending on their unique features, and group the requirements into the following settings; identity management, network security, resilience and trust, and lastly privacy. The authors in this case specifically consider numerous architectures that have widely been proposed for the internet of things within the research community and make an analysis of whether several architectures tend to meet the required security measures. The critical analysis demonstrates that several security needs are seriously considered though none of all the architectures covers all of the security needs [45].

The most uncovered are the trust and privacy requirements. As long as there exist computers, there exist a perfectly accepted model for the information technology security based on the most desired security features, usually abbreviated as CIA, confidentiality (such as trying to prevent any form of unauthorized access to the relevant data), integrity (trying to make sure that the data given is not altered in any way), and lastly, availability (making sure that data can be accessed any time it is needed) [45].

These three properties have been deeply described in a form of a triangle within which properties are placed at the vertices. Through the decades, the model has been modified with several possible main properties, though the very main properties, CIA,

have remained over time. Something which is yet to be fully highlighted is the fact that such three properties cannot be achieved fully in a simultaneous manner, as they are considered to be mutually exclusive. For example, provided with the same amount of resources, it is not possible to increase the overall availability, without compromising the accuracy, confidentiality or even both. For the general information-processing computer systems, traditional security has mainly focused on the overall confidentiality of the said property, though for a number of the systems which are embedded as well as the IoT, one can make an argument that the other two aspects are the most crucial ones, or even much more essential that it is within the office information system [38]. The other important observation is that the variance in the approach I most of the cases seriously impact on cooperation which is there between the standard IT systems and administrators of the control system.

Whetstone & Goldsmith [61] confirmed that the confidence of an individual regarding the privacy and security of their medical records had a positive influence on their morale to establish an electronic health record. Bansal et al. [11] confirmed that concerns regarding privacy negatively impacted the intentions to share their health information online. Another research that was conducted by Anderson & Agarwal [8] established that there existed a negative effect of health information privacy concerns on how willing the individuals would cooperate in providing access to personal health information. On the other hand, Dinev et al. [22] found out the existence of a poor relationship between concerns of people's health information privacy and their attitude towards electronic health records. Angst & Agarwal [9] also had the same conclusion regarding the acceptance of electronic health records. A study conducted by Ermakova et al. [25] showed that concerns on health information privacy reduced the willingness of patients to allow health care providers share their medical data while using cloud computing technique. The existence of privacy concerns makes trust to become more vital than the discounts when choosing a healthcare except for the case of secondary use. Kuo et al. [44] carried out a study whose results confirmed that there were existing concerns regarding health information privacy on the information privacy-protective responses (IPPR) such as refusal of patients to give their personal information to health care providers, fabricating personal information of patients to medical facilities, requesting for the removal of personal information of patients, negative utterances to their friends, complaints issued directly to the medical facilities, complaints issued in an indirect way to a third-party organization.

Rohm and Milne [54] established that consumers' concerns increases if an organization acquired a list containing individual medical history as compared to a list containing general information. There was also a study by Zulman et al. [64] that reported that preferences of individuals regarding sharing of their electronic health information vary depending on the kind of information that is subject to undergo sharing. King et al. [40] also realized that matters concerning privacy vary for specific items of health records. It was confirmed that items in the health facility that people have more concern about include infertility issues, abortion, sexually transmitted diseases among other issues that directly affected their families. People showed a relatively lower privacy concerns for some of their information on the health records such as religion, date of birth, blood group, language, gender, status of blood pressure and cancer status.

## 3. Security and privacy features of current EHR systems

The three security-safeguard themes namely physical, technical and administrative have been applied in the analysis of a number of research. These themes consist of a number of security strategies used by healthcare administrations to provide more security to the secured health information that is in the electronic health records. The theme of administrative safeguard is the first safeguard that comprise of relevant techniques like performing audits, employing an officer in charge of information security, and coming up with contingency plans [62]. This theme have got safeguards that focuses on having a compliant security procedures and policies. The other theme is physical safeguards which includes techniques listed in organizational safeguards and in addition, it focuses on protecting the health information physically so that their software or hardware are not accessed by unauthorized persons or those who could misuse them [62]. Breaching of physical safeguards is among the major contributor of security ruptures ranked second overall [47]. Examples of techniques under physical safeguards include having assigned security roles [46].

Technical safeguards are the third category of themes and they carry out protection of the whole information system found in the network of a health organization [47]. This theme is very essential in ensuring the security of the organization because most breaches to security happen via the electronic media through the use of computers and other transferrable electronic devices [47]. This theme have got security techniques such as the use of firewalls and encryption, virus checking and measures used in authenticating information[46]. However, it was concluded by Lemke [46] that firewalls and cryptography were the most applied security techniques. Other notable security techniques that are also used included antivirus software, chief information security officers and cloud computing though their implementation are dependent on the budget [27].

From the research by Liu et al. [47], it was realized that there are physical safeguard such as physical access control that are used to prevent theft such as the use of locks on computers together with technical safeguards to prevent electronic breaches through use of firewalls and encryption. Amer [6] carried out a study on informatics through ethical application of genomic information and electronic health records. He realized that encryption could provide technical safeguard while administrative safeguards used a security technique of de-identifying samples collected or the research. Technical safeguards can also be implemented through firewalls; encryption and decryption while administrative safeguard was tackled through implementing comprehensive education and security plans and employing a Chief Information Security Officer [37]. Wikina [62] mentioned that administrative safeguards involved a manager approving the release of paper data containing information of patients and carrying out trainings on how to respond to missing records while physical safeguards involved installation of security cameras.

There are more advancing in the modern technology, healthcare organizations are as well continuingly being targeted for breaching security. It is very important for organizations to stick to new technology and threats and have taken management of risk very seriously, including the Clinical Engineering Information Technology Community; the American College of Clinical Engineering; and the Healthcare Information and Management Systems Society among other organizations [37]. The above listed steps of risk assessment and management together with the named organizations ensures that the healthcare organization are advanced in fortifying patients information within electronic health records. Healthcare institutions recognizing the advantages of security and privacy as a result of applying RFID are growing. Some examples of the RFID techniques include storage of data within RFID tags and creating restrictions for accessing RFID tags. These techniques have improved privacy and security through restrictions that allows only the few authorized individuals to access the information [37]. Making good use of a Chief Information Security Officer

can help in managing and coordinating all the security methods and initiatives in electronic health records [37].

Firefox use is one of the technologies that are used to provide protection to the information technology systems of healthcare organizations [18,19]. Firefox are very effective in securing the network of an organization and ensuring that the health information is protected on the existing network. Firefox is used both inside and outside when protecting the business from threats that could interfere with its information network. They come in different forms [47].

The use of level gateway is the third category of firewalls. They play a role of gatekeeping for the network of the organization when the IP web page is being scanned for any threats before passing the web page to the end users. The external network connections of status inspection firewalls are accessible via the gateway so that the entry of external networks into the organization's intranet is prevented [47]. Submission equal gateways have successfully secured electronic health records because they block hackers from directly entering the system and reach the health information which is protected. This group of firewalls is not easy to be applied by organizations because of their complexity and high costs involved and it is therefore necessary that both external and internal analysis of the entire organization be conducted to find out if the firewall is applicable and viable for every organization. Finally, we have a group of firewalls referred to as the network address translator. It helps by hiding the organization's intranet IP addresses so that they are not accessed by external users that could have plans to create damages [47]. Network address translator establishes a barrier among an organization's intranet as well as the local area networks. Although firewalls are very effective in ensuring that the electronic health records are secure, it is still very essential that all the four steps of its refuge strategies are applied. The order of the steps include service control, direction control, user control, and behavior control [62]. Generally, it is important that the organization does a complete needs assessment, budgetary assessment and threats assessment both external and internal to the organization prior to using any form of firewall. Failure of an organization to do the above assessments or incompletion of the four security plans can negatively affect the security of patients' electronic health records or even the entire information system of the organization [18,19].

Cryptography has been used as a way of securing or protecting the electronic health records. The use of encryption has increased the security of electronic health records during the process of exchanging health information. The process of exchanging health information has got specifications to be followed through criteria that normally require recording of the exchange procedure to be done by organizations when the encryptions are either enabled or dsabled [60]. The Health Insurance Portability and Accountability Act (HIPAA) designed ways by which cryptography could be used to secure health information [20]. HIPAA broadened its standards on security in 2003 when the United States Department of Health and Human Services formed the Concluding Rule [58]. The Concluding Rule enabled HIPAA to expand the organizations' ways of making, receiving, keeping and sending of health information that is protected (PHI) [58]. Decryption has been useful in ensuring that the electronic health records of patients are secure [62]. The use of digital signatures have solved the problem of breaching protected health records when patients check their personal information. Digital signatures have effectively been applied to prevent security breaches.

Electronic health records become much more accessible and secure through safeguarding mobile agents for patients data that are transmitted from one facility to the other [46]. Use of usernames is another form of cryptography. They can help in preventing security breaches through integrating individual privacy on passwords and advocating that the password users change these passwords frequently [46]. Names commonly used and dates must be avoided to prevent chances of a hacker speculating the set password. Applying username and password security technique are useful in the case of achieving controls. The role-based controls to perform restriction on access of data to users through applying usernames and passwords created by system administrators. This technique does not offer effective protection of information within electronic health records from internal threats [46]. Logging from the system by employees must be done once they are through in order to ensure that the dwindling health facts in a condition that the unauthorized persons can see [46].

Other commonly used security technique include installation of antivirus software, cloud computing, preliminary risk assessment sequencers, employment of a chief information security officer and radio frequency identification (RFID) [43,50]. Remote Patient Monitoring (RPM) is another new technology that is being used to ensure there is privacy and security of the records in an electronic health records. In this case, different types of sensors are used to perform the monitoring of patients' important signs while at home. They use sensors that can be worn or implanted. These sensors sends information through wireless communication to a local base station that is located within the patient's residence. The station ensures that the information is evaluated and signals a central monitoring station when there are differences from the set normal limits. The healthcare provider is then able to take necessary actions once alarmed in helping the patient. Some of the conditions that the Remote Patient Monitoring technology is most suitable include dementia, diabetes and congestive heart failure. Implementing these new technologies can result into many advancements in the healthcare sector, it can also interfere with the privacy of individuals despite regulations such as the Health Insurance Portability and Accountability Act (HIPAA). The data of electronic heath records is communicated electronically via Internet or wireless connections and hence threats such as eavesdropping, data theft and data misuse can be experienced. Eventually, challenges such as severe social implications, e.g. employers failing to hire or fire their employees because of their medical conditions and insurance firms refusing to offer insurance to patients.

The increasing use of technology has led to massive research conducted on cloud computing for integration into the EHR systems. The infrastructure created by cloud computing enables one to perform electronic assignment and information sharing the "renting" of storage, as well as computing power. This way, the healthcare institutions are in a position to spend less on establishing an EHR system via moving ownership avoiding the maintenance cost, while at the same time incorporating cryptography procedures [43]. Even though cloud computing platform looks promising, antivirus software is a more commonly applied security measure. Achampong [1] also indicates that security issues that come from IT trends such as hosting health records on distant serves operated by third-party cloud service providers [33].

The HITECH Act emphasized on the need to always report data breaches in 2009 and the specific protocol that should be used when reporting data breaches; for instance the Act require that the entity issues specific details in case of a data breach of more than 500 people [62]. Through the HITECH Act, the Centers for Medicare and Medicaid Services (CMS) beneficiaries were mandated to make use of EHRs not later than 2015 so as to get full reimbursements. There were presents that were given to those who made use the EPR by 2015 and who failed to meet the deadline suffered penalties. The Office of the National Coordinator (ONC) established the three "meaningful use" stages that were supposed to be implemented by healthcare bodies using EHRs. Meaningful use evaluates the level at which an entity is making use of EHRs when compared to the earlier documentation methods [47].

Due to IT-related security concerns that have always been raised over time, health care providers implementing HIT are required to establish an adequate security system. This system is a set of security mechanisms that should be done in accordance with a security policy which normally contains legislations that allow or deny possible actions, events, or anything that relates to security [10]. Generally, an Information Technology security policy ensures that the IT assets of an organization including data, people, hardware and software are confidential, have integrity, and are available to the required standards [53].

## 4. Information technology security incidents in health care settings

Infosec Institute reported that the remarkable growth in the adoption of electronic health records in the recent years has not been protected by establishment of a cyber-security measure, thus subjecting the health care industry to a lot of damages from cyber threats [51]. This report got a lot more support from other reports of Information Technology related incidents that were experienced in hospital settings. A finding from Information Security Media Group (2014), established that at least one security breach that affects less than 500 individuals has been reported in 75% of surveyed health care organizations in the US, and at least one incident affecting more than 500 individuals was reported by 21% of surveyed health care providers [30]. The Healthcare Information and Management Systems Society (2015) realized that 68 percent of surveyed health care organizations in the US submitted that they had recently experienced a significant security incident [32]. These reported security incidents were from both insider threats (53.7%) and external threats (63.6% of health care organizations) [32].

The IT related security breaches could be more than the reported cases considering that there are other incidences that go undetected or poorly assessed [30], together with the likelihood of organizations to underreport security incidents [48]. There are documentations showing that security breaches in healthcare can be very costly; for instance, Absolute Software Corporation which reported that cases of breaches in health care data costs hospitals as high as US $250,000 to US $2.5 million in settlement payments. This represent but a fraction of the overall financial burden of the incidents [30]. Concerns of security and privacy together with fear of related liabilities hinders healthcare providers from using information and technology in improving their services. It is therefore critical that organizations improve their HIT security and privacy practices in the healthcare facilities as a measure to ensure that an effective health care is provided. Liu, Musen & Chou [47] explained that the security and privacy concerns can be addressed by organizations willing to apply information and technology in improving their healthcare services by putting in place IT security measures that are in line with their information and technology development plans. However, some studies have identified insider threats very difficult to address when compared to external threats because internal threats are done by individuals who are authorized personnel and therefore identifying the criminal becomes very difficult.

The Information and Communication Technologies (ICT) have assisted patients in transforming their roles from just being the traditional passive receivers of healthcare services into a more active role of understanding their health records and make choices and take part in decision making process [63]. This has increased the challenges of the level of freedom that should be granted to issuers and data subjects. There are a number of solutions to some of the identified challenges by implementing privacy and security together with accountability and key management in electronic health record technology. In the recent past, the issue of security and privacy has resulted to a lot of concerns in implementation of electronic health records.

## 5. Conclusion and future work

The present work has performed a literature review related to the security and the privacy of electronic health record systems. The paper has analysed different security and privacy and issues that arise from the use of EHRs and looks at the potential solutions. It is evident from the literature that Electronic Health Records allows the structure medical data to be shared easily among the authorized healthcare providers so as to improve the overall quality of the healthcare services delivered to the patients. The use of e-health enables the users to have a wider thinking and allows health care providers to network effectively.

Electronic health records allow the medical information to be shared amongst stakeholders very easily and the patient information be accessed and updated as a patient undergoes treatment. In such systems, however, security and privacy concerns are very much essential, based on the fact that the patient might face serious problems if sensitive information is disclosed to a third party. From the articles reviewed and based on the security areas analysed, it is evident that different regulations and standards related to privacy and security are used in the electronic health records. However, there is need for such systems to be harmonized so as to resolve possible conflicts and inconsistencies among standards. Numerous encryption algorithms have been proposed by various articles.

It is highly recommended that efficient encryption scheme that can easily be applied by both the healthcare professionals and the patients be applied on the latest EHR records. The preferred access control model in the electronic health record systems is RBAC while the best authentication mechanisms are passwords/logins and digital signature. Effectively managing an electronic-health record requires multidisciplinary team including telecommunication, instrumentation and computer science to enable exchange of medical data across wider geographic regions.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgements

The authors would like to acknowledge the support provided by AlMaarefa University while conducting this research work.

## References

[1] Achampong E. Electronic health record (EHR) and cloud security: the current issues. IJ- CLOSER 2014;2(6):417–20.
[2] Alanazi HO et al. Meeting the security requirements of electronic medical records in the ERA of high-speed computing. JMed Syst 2015;39(1):165.
[3] Albahri OS et al. Systematic review of real-time remote health monitoring system in triage and priority-based sensor technology: taxonomy, open challenges motivation and recommendations. J Med Syst 2018;42(5):80.
[4] Allard T, Anciaux N, Bouganim L, Guo Y, Folgoc LL, Nguyen B, et al. Secure personal data servers: a vision paper. PVLDB 2010;3(1–2):25–35.
[5] Alsalem MA et al. Systematic review of an automated multiclass detection and classification system for acute leukaemia in terms of evaluation and benchmarking, open challenges, issues and methodological aspects. J Med Syst 2018;42(11):204.
[6] Amer K. Informatics: ethical use of genomic information and electronic medical records, J Am Nurses Assoc 2015;20(2).
[7] Ancker J, Silver M, Miller M, Kaushal R. Consumer experience with and attitude toward health information technology: a nationwide survey. Am Medical Informatics Assoc 2012;1:152–6.

[8] Anderson C, Agarwal R. The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information. Information Syst Res 2011;22(3):469–90.
[9] Angst C, Agarwal R, Downing J. An empirical examination of the importance of defining PHR for research and for practice. Robert H. Smith School Research Paper No. RHS-06-011; 2006.
[10] Bahtiyar Ş, Çağlayan MU. Trust assessment of security for e-health systems. Electron Commer Res Appl 2014;13(3):164–77. doi: https://doi.org/10.1016/j.elerap.2013.10.003.
[11] Bansal G, Zahedi F, Gefen D. The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decis Support Syst 2010;49(2):138–50.
[12] Benaloh J, Chase M, Horvitz E, Lauter K. Patient controlled encryption: ensuring privacy of electronic medical records. In: Proc ACM workshop on cloud computing security; 2009, p. 103–14.
[13] Brumen B, Heričko M, Sevčnikar A, Završnik J, Hölbl M. Outsourcing medical data analyses: can technology overcome legal, privacy, and confidentiality issues? J Med Internet Res 2013 Dec 16;15(12):e283 [FREE Full text] [CrossRef] [Medline].
[14] Carey DJ, Fetterolf SN, Davis FD, Faucett WA, Kirchner HL, Mirshahi U, et al. The Geisinger MyCode community health initiative: an electronic health record–linked biobank for precision medicine research. Genet Med 2016;18(9):906.
[15] Centers for Medicare & Medicaid Services. Electronic Health Records. URL: https://www.cms.gov/Medicare/E-health/EHealthRecords/index.html.
[16] Chen C-L, Huang P-T, Deng Y-Y, Chen H-C, Wang Y-C. A secure electronic medical record authorization system for smart device application in cloud computing environments. Human-Centric Computing Information Sci. 2020;10:1–31.
[17] Cifuentes M, Davis M, Fernald D, Gunn R, Dickinson P, Cohen DJ. Electronic health record challenges, workarounds, and solutions observed in practices integrating behavioral health and primary care. J Am Board Fam Med 2015;28 (Supplement 1):S63–72.
[18] Collier R. New tools to improve safety of electronic health records. CMAJ 2014;186(4):251. doi: https://doi.org/10.1503/cmaj.109-4715. [PMC free article].
[19] Collier R. US health information breaches up 137%. Can Med Assoc J 2014;186 (6):412. doi: https://doi.org/10.1503/cmaj.109-4731.
[20] Cooper T, Fuchs K. Technology risk assessment in healthcare facilities. Biomed Instrum Technol 2013;47(3):202–7. doi: https://doi.org/10.2345/0899-8205-47.3.202.
[21] Dehling T, Sunyaev A. Secure provision of patient-centered health information technology services in public networks—leveraging security and privacy features provided by the German nationwide health information technology infrastructure. Electron Markets 2014;24(2):89–99.
[22] Dinev T, Albano V, Xu H, D'Atri A, Hart P. Individual's attitudes towards electronic health records – a privacy calculus perspective. Ann. Information Syst. 2012.
[23] Dorgham O, Al-Rahamneh B, Almomani A, Khatatneh KF. Enhancing the security of exchanging and storing DICOM medical images on the cloud. Int. J. Cloud Appl. Computing (IJCAC) 2018;8(1):154–72.
[24] Edemekong PF, Haydel, MJ, 2018. Health Insurance Portability and Accountability Act (HIPAA).
[25] Ermakova T, Fabian B, Zarnekow R. Security and Privacy System Requirements for Adopting Cloud Computing in Healthcare Data Sharing Scenarios. Proceedings of the 19th Americas Conference on Information Systems, 2013.
[26] Gupta BB. Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives. In: Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives. CRC Press, Taylor & Francis; 2018, p. 666.
[27] Gupta BB, Agrawal DP, (Eds.). Handbook of Research on Cloud Computing and Big Data Applications in IoT, IGI GlobalHershey; 2019.
[28] Haque Rafita, Hasan Sarwar, Rayhan Kabir S, Rokeya Forhat, Muhammad Jafar Sadeq, Md Akhtaruzzaman, Nafisa Haque, Blockchain-Based Information Security of Electronic Medical Records (EMR) in a Healthcare Communication System, In: Intelligent Computing and Innovation on Data Science, Springer, Singapore, 2020, pp. 641–650.
[29] Häyrinen K, Saranto K, Nykänen P. Definition, structure, content, use and impacts of electronic health records: a review of the research literature. Int J Med Inform 2008;77(5):291–304.
[30] Healthcare Information Security. Princeton, NJ: ISMG; 2014. The State of Healthcare Information Security Today. Update on HIPAA Omnibus Compliance, Protecting Patient Data URL: https://www.healthcareinfosecurity.com/surveys/state-healthcare- information-security-today-s-23 [accessed 2019-02-04]
[31] Hesse BW, Hansen D, Finholt T, Munson S, Kellogg W, Thomas JC. Social participation in health 2.0. Computer 2010;43(11):45–52.
[32] HIMSS. Chicago, IL: HIMSS; 2015 Jun. 2015 HIMSS Cybersecurity Survey URL: https://www.himss.org/2015-cybersecurity-survey/full-report [accessed 2019-02-04]
[33] Hunter ES. Electronic health Records in an Occupational Health Setting-Part I. A global overview. Workplace Health Safety 2013;61(2):57–60.
[34] Hussain M et al. A security framework for mHealth apps on Android platform. Comput Secur 2018;75:191–217.
[35] Hussain M et al. The landscape of research on smartphone medical apps: coherent taxonomy, motivations, open challenges and recommendations. Comput Methods Prog Biomed 2015;122(3):393–408.
[36] Ives TE. The New 'E-Clinician' guide to compliance. Audiol. Today. 2014;26 (1):52–3. [Google Scholar]
[37] Jannetti MC. Safeguarding patient information in electronic health records. AORN J 2014;100(3):C7–8. doi: https://doi.org/10.1016/S0001-2092(14)00873-4.
[38] Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D. Security of the Internet of Things: perspectives and challenges. Wireless Netw 2014;20(8):2481–501.
[39] Kiah MLM et al. MIRASS: medical informatics research activity support system using information mashup network. J Med Syst 2014;38(4):37.
[40] King T, Brankovic L, Gillard P. Perspectives of Australian adults about protecting the privacy of their health information in statistical databases. Int J Med Informatics 2011;81:279–89.
[41] Kisekka V, Giboney J. The effectiveness of health care information technologies: evaluation of trust, security beliefs, and privacy as determinants of health care outcomes. J Med Internet Res 2018;20(4):e107.
[42] Kruse CS, Beane A. Health information technology continues to show positive effect on medical outcomes: systematic review. J Med Internet Res 2018;20 (2):e41.
[43] Kruse CS, Smith B, Vanderlinden H, Nealand A. Security techniques for the electronic health records. J Med Syst 2017;41(8):127.
[44] Kuo K-M, Ma C-C, Alexander J. How do patients respond to violation of their information privacy. Health Information Manag J 2013;43(2):23–33.
[45] Lafky D, Horan T. Personal health records: consumer attitudes toward privacy and security of their personal health information. Health Informatics J 2011;17 (1):63–71.
[46] Lemke J. Storage and security of personal health information. OOHNA J 2013;32(1):25–6.
[47] Liu V, Musen MA, Chou T. Data breaches of protected health information in the United States. J Am Med Assoc 2015;313(14):1471–3. doi: https://doi.org/10.1001/jama.2015.2252 [PMC free article] [PubMed] [CrossRef] [Google Scholar].
[48] Ma Q, Schmidt MB, Pearson JM, Herberger GR. An integrated framework for information security management. Rev Bus 2009;30(1):58–69.
[49] Miotto R, Li L, Kidd BA, Dudley JT. Deep patient: an unsupervised representation to predict the future of patients from the electronic health records. Sci Rep 2016;6:26094.
[50] Muhammad G, Alhamid MF, Alsulaiman M, Gupta B. Edge computing with cloud for voice disorder assessment and treatment. IEEE Commun Mag 2018;56(4):60–5.
[51] Paganini P. Infosec Institute. 2014. Risks and cyber threats to the healthcare industry URL: https://resources.infosecinstitute.com/risks-cyber-threats-healthcare-industry/ [accessed 2018-06-01] [WebCite Cache]
[52] Perera G, Holbrook A, Thabane L, Foster G, Willison DJ. Views on health information sharing and privacy from primary care practices using electronic medical records. Int J Med Informatics 2011;80(2):94–101.
[53] Pfleeger CP, Pfleeger SL, Margulies J. Security in computing. In: Security In Computing (5th Edition). Upper Saddle River, NJ: Prentice Hall; Feb 5, 2015:944.
[54] Rohm A, Milne G Just. What the doctor ordered. The role of information sensitivity and trust in reducing medical privacy concern. J Business Res 2004;57:1000–11.
[55] Rothstein MA. Health privacy in the electronic age. J Leg Med 2007;28 (4):487–501.
[56] Sheikh A, Sood HS, Bates DW. Leveraging health information technology to achieve the "triple aim" of healthcare reform. J Am Med Inform Assoc 2015;22 (4):849–56.
[57] Sittig DF, Singh H. A new socio-technical model for studying health information technology in complex adaptive healthcare systems. In: Cognitive Informatics for Biomedicine. Cham: Springer; 2015. p. 59–80.
[58] Tejero A, de la Torre I. Advances and current state of the security and privacy in electronic health records: survey from a social perspective. J Med Syst 2012;36 (5):3019–27. doi: https://doi.org/10.1007/s10916-011-9779-x.
[59] Verheij RA, Curcin V, Delaney BC, McGilchrist MM. Possible sources of bias in primary care electronic health record data use and reuse. J Med Internet Res 2018;20(5):e185.
[60] Wang CJ, Huang DJ. The HIPAA conundrum in the era of mobile health and communications. JAMA 2013;310(11):1121–2. doi: https://doi.org/10.1001/jama.2013.219869.
[61] Whetstone M, Goldsmith R. Factors influencing intention to use personal health records. Int J Pharmaceutical Healthcare Marketing 2009;3(1):8–25.
[62] Wikina SB. What caused the breach? An examination of use of information technology and health data breaches. Perspect Health Inf Mana 2014;2014:1–16.
[63] Win KT. A review of security of electronic health records. Health Information Manag. 2005;34(1):13–8.
[64] Zulman DM, Nazi KM, Turvey CL, Wagner TH, Woods SS, An LC. Patient interest in sharing personal health record information. Ann Intern Med 2011;155 (12):805–11.