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 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

Please cite this article as: I. Keshta and A. Odeh, Security and privacy of electronic health records: Concerns and challenges, Egyptian Informatics Journal, https://doi.org/10.1016/j.eij.2020.07.003

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

Please cite this article as: I. Keshta and A. Odeh, Security and privacy of electronic health records: Concerns and challenges, Egyptian Informatics Journal, https://doi.org/10.1016/j.eij.2020.07.003

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.