Egyptian Informatics Journal xxx (xxxx) xxx

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 xxxx

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

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

[*] 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.

ELSEVIER Production and hosting by Elsevier

https://doi.org/10.1016/j.eij.2020.07.003
1110-8665/© 2020 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University.

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 doctors 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].

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

[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.