How to Cite:
Alonayzan, H. H. M., Alenezi, Talal S. S., Alshammari, Khalaf S. F., Albakr, Mohammed S. B., Alshammari, Sanad H. S., Alghadeer, Saleh O. A., Alshammari, Nezar M. M., Almughamis, Fahad K. S., Alanzi, Nuri R., Hamran, Abdullah I., Al-Sharari, Fawaz A., Alotaibi, A. T., Alanzi, A. S. B., Aldhafiri, Mohammed F., & Sadi, A. J. (2018). The potential of voice recognition technology in medical record documentation: Review. *International Journal of Health Sciences*, *2*(S1), 17–31. https://doi.org/10.53730/ijhs.v2nS1.14933

The potential of voice recognition technology in medical record documentation: Review

Hamad Hassan Mohammed Alonayzan
KSA, National Guard Health Affairs
Email: Alonizanha@ngha.med.sa

Talal Sanian Salem Alenezi
KSA, National Guard Health Affairs
Email: Alenezyta@ngha.med.sa

Khalaf Saud Faryhan Alshammari
KSA, National Guard Health Affairs
Email: alshammarykh@ngha.med.sa

Mohammed Saad Bakr Albakr
KSA, National Guard Health Affairs
Email: al-bakrmo@ngha.med.sa

Sanad Hamdan Sanad Alshammari
KSA, National Guard Health Affairs
Email: aIshammarisa5@ngha.med.sa

Saleh Obaid Abdullah Alghadeer
KSA, National Guard Health Affairs
Email: Alghadersa@ngha.med.sa

Nezar Mohammad Mutlaq Alshammari
KSA, National Guard Health Affairs
Email: Alshammaryne@ngha.med.sa

Fahad Khalifah Salem Almughamis
KSA, National Guard Health Affairs
Email: almgamasfa@ngha.med.sa

Nuri Rawafa Alanzi
KSA, National Guard Health Affairs
Email: alenazinu@ngha.med.sa

International Journal of Health Sciences E-ISSN 2550-696X © 2018.
Manuscript submitted: 09 Sept 2018, Manuscript revised: 18 Oct 2018, Accepted for publication: 27 Nov 2018

Abdullah Ibrahim Hamran
KSA, National Guard Health Affairs
Email: Hamranab@ngha.med.sa

Fawaz Ayed Al-Sharari
KSA, National Guard Health Affairs

Ahmed Turki Alotaibi
KSA, National Guard Health Affairs
Email: A7mdoh85@gmail.com

Awad Shehab B Alanzi
KSA, National Guard Health Affairs

Mohammed Farhan Aldhafiri
KSA, National Guard Health Affairs

Almatrafi Jaber Sadi
KSA, National Guard Health Affairs

***Abstract*---**Background: Electronic health records (EHRs) have become an integral part of healthcare, providing a digital representation of patient medical histories. However, the transition from paper-based to electronic records has raised concerns about the security and privacy of sensitive health data. Aim of Work: This study aims to provide valuable insights to stakeholders in the healthcare system on the need for implementing, selecting, developing, and using electronic health records that improve the privacy and security of patients. Methods: The review explores the potential of voice recognition technology in medical record documentation, examining the key security and privacy considerations surrounding electronic health records. Results: The study highlights the importance of ensuring the confidentiality, integrity, and availability of health data stored in electronic systems. It also discusses the impact of emerging technologies, such as cloud computing and mobile devices, on the security and privacy of electronic health records. Conclusion: Securing electronic health records is crucial to safeguarding patient privacy and maintaining trust in the healthcare system. The study emphasizes the need for a multidisciplinary approach involving experts in communications, instrumentation, and computer science to facilitate the secure exchange of medical data and enhance the overall quality of healthcare services.

***Keywords*---**Electronic Health Records, Security, Privacy, Voice Recognition, Healthcare, Information Technology.

Introduction

An electronic health record (EHR) is a digital representation of a patient's medical history maintained by a healthcare provider. It contains comprehensive administrative and clinical data related to the care provided by a specific provider, including demographics, progress reports, problems, medications, vital signs, medical history, immunization records, laboratory data, and radiology reports [1-4]. The use of paper for documenting health data in healthcare institutions and organizations has resulted in a significant accumulation of paper records. Consequently, many organizations are now inclined towards transitioning from paper-based health records to electronic health records. According to Carey et al. [5], integrated health records are very successful and provide several advantages, including cost reduction, improved healthcare quality, increased use of evidence-based treatment, streamlined record keeping, and enhanced mobility of information. In order to maintain effectiveness, an electronic health record system must meet certain criteria, including ensuring the presence of comprehensive data, being resilient to failures, maintaining high availability, and adhering to security regulations [6-8]. Nevertheless, many problems have impeded the use of electronic health records. The elements include financial support for technology, certain facets of the organization, and mindset.

Electronic Health Records, often known as electronic medical records (EMR), are increasingly being used in the field of e-health [1]. Electronic medical records store and organize health-related information of patients, and are considered a significant component of e-health implementation. An electronic medical record consists of legally binding records that are created inside hospital settings. Subsequently, this data serves as the primary data source for electronic health record [1]. Despite the use of electronic medical records systems in hospitals' daily operations, healthcare professionals' lack of complete faith in the system is attributed to their extensive expertise. According to Albahri [3], the term e-health emerged in the early 21st century and refers to the use of advanced information and communication technologies to provide medical services in the healthcare industry. An efficient management of an Electronic-health system necessitates a multidisciplinary team of experts in communications, instrumentation, and computer science. This team is responsible for facilitating the interchange of medical data over larger geographic areas [9]. Utilizing e-health expands consumers' cognitive abilities and enhances the networking capabilities of healthcare professionals [10-14]. Enhancing healthcare yields advantages such as optimizing the efficiency of healthcare operations and enhancing the quality of healthcare services provided to patients.

Aim of the Study

This study has the potential to provide valuable insights to stakeholders in the healthcare system and other agencies on the need of implementing, selecting, developing, and using certain Electronic Health Records that improve the privacy and security of patients. This document is intended for custodians who are responsible for supervising the security and privacy of information systems in the healthcare industry. The study may serve as a valuable resource for other academics seeking to increase the security and privacy of patients in electronic health record systems.

Electronic Medical Record

Electronic health records refer to distinct concepts that include patients' health-related information and serve as the foundation for e-health applications [15-20]. These data are very valuable for all healthcare providers. Electronic health records provide seamless sharing of medical information across stakeholders, enabling easy access and updating of patient information throughout the course of treatment. According to Alsalem et al. [5], health information technology has the potential to significantly enhance efficiency, patient safety, and healthcare outcomes, while simultaneously cutting costs. Electronic Health Records (EHRs) provide advantages such as cost savings via the digitization of data systems and the establishment of a centralized repository for medical information [5,21,22]. However, health statistics have mostly relied on paper-based data for an extended period of time. Nevertheless, significant transformations have occurred in the last thirty years due to the growing use of health information technology.

Literature has addressed security concerns arising from the emergence of information and technology trends, such as the practice of storing health data on remote servers managed by third-party cloud service providers [1,23]. Health Information Technology encompasses the many information technology systems used for the purpose of storing, accessing, processing, exchanging, and transferring health information, as well as supporting healthcare delivery and healthcare system administration [24-27]. The Health Information Technology contains very sensitive information, including data on patient testing, diagnosis, treatment, and medical history [16, 28, 29]. It is crucial to ensure the security of this information to prevent any manipulation, allowing patients to freely share their health and work-related information while upholding moral and legal obligations. However, the dynamic nature of the Health Information Technology environment [30] has a detrimental impact on the ability to ensure the security of health data.

The primary concerns that must be resolved in an electronic medical record system are privacy, security, and confidentiality [2]. While security and privacy are closely interconnected, they are fundamentally distinct. Privacy is the individual's right to control the transfer or sharing of their personal information, including when and how it is accessed by others. On the other hand, security refers to the level of restriction placed on accessing someone's personal information, allowing only authorized individuals to do so [26, 31]. Unauthorized transfer or exchange of sensitive health data might result in a data breach. Privacy may be compromised in several scenarios due to unavoidable systemic identification across the complete electronic health infrastructure, as well as by central technologies and entities that monitor the activities of healthcare professionals and patients [32]. However, there are instances where the government, employers, pharmaceutical companies, researchers, and laboratories may have legitimate justifications for accessing patients' health records in order to obtain data. In doing so, there is a possibility that healthcare providers may unintentionally or deliberately misuse their access to these records [17].

Dehling and Sunyaev [21] proposed that the fundamental security criteria for information technology are confidentiality, integrity, and availability. Confidentiality refers to the act of limiting access to data to only authorized individuals during storage, transmission, or processing. Confidentiality may be ensured by using technical measures like data encryption or by regulating access to the systems. Confidentiality is also attained by cultivating ethical qualities such as professional discretion [13]. However, it was observed by [21] that although encryption is often used for securing health data sent across vulnerable networks, it is less frequently utilized for protecting data saved on mobile devices and other storage media. The need for secrecy arises from the imperative to address privacy issues, which are particularly crucial in the healthcare industry owing to the very sensitive nature of the data pertaining to patients and customers that it handles. Dehling and Sunyaev [21] said that confidentiality guarantees the protection of information against unlawful deletion, modification, and undesirable alteration by authorized users. Conversely, availability guarantees that a system may be accessed and is fully functional whenever an authorized individual requires its use. Availability encompasses several factors, including scalability, resilience, and data recoverability in the event of data loss [21].

Physicians are typically highly concerned about the potential for unauthorized individuals to access and misuse patient information stored in the electronic medical records system, which could result in legal complications due to a breach in patient record confidentiality [33]. According to Wikina [34], doctors prioritize security and confidentiality issues more than the patients themselves. Most clinicians who use electronic medical records have a greater preference for paper records due to their perception of enhanced security and confidentiality. This demonstrates a strong commitment to addressing the concerns of privacy and security on EMR. In the absence of guaranteed privacy, patients may choose to conceal information in order to avoid its improper use [35-41].

Several nations are now undergoing health care service reforms by using Information Technology [42]. Utilizing information technology (IT) has facilitated patients in enhancing their care experience, improving the overall health of the community, and reducing healthcare expenses [43]. The advancements in Information Technology have led to the digitization of health records, hence enabling new and enhanced methods for effectively collecting, processing, storing, accessing, and exchanging health information. Digitized health information is very portable and may be easily shared throughout healthcare institutions. It is readily accessible to public health officials for conducting health surveys and setting policy. Additionally, it is also accessible to patients. Existing evidence overwhelmingly supports the notion that a digitalized system has good benefits on healthcare outcomes [42]. Nevertheless, the digitalization of health information increases the vulnerability of health data to security breaches associated with information technology. Prospective users of health Information Technology are greatly worried about the security and privacy issues associated with information technology, which has a negative impact on the confidence in electronic health records. The diminished confidence among healthcare professionals and patients may hinder the acceptance of electronic health records, thereby jeopardizing the significance of information technology [43]. This may then result in inefficient healthcare provision [41] as well as inadequate public health surveillance or health research [44-47].

Liu et al. [48] have proposed that a thorough understanding of the approaches for ensuring cyber-security in electronic health records is crucial before implementing them. The data kept in the EHR is very sensitive, prompting the implementation of several security measures by the Health Information Technology for Economic and Clinical Health Act and the Health Insurance Portability and Accountability (HIPAA) Act [24]. HIPAA employs three key principles to ensure the security of protected health information: administrative safeguards, physical safeguards, and technology safeguards [36]. The three pillars, also known as the healthcare security safeguard themes, include various approaches to secure the location of computers and the use of firewall software to preserve health information [49-51].

It is worth mentioning that electronic health records (EHR) are becoming more widely used in some developing countries due to their ability to enhance healthcare quality and provide cost-effective solutions. Technologies of this kind might pose risks, therefore making it a significant task to ensure the security of the information stored inside the system. Recent security breaches have prompted questions over the integrity of this system [52-55]. Despite its increasing usefulness and rising excitement for its adoption, there has been little focus on the potential security and privacy concerns that may develop. Hence, the authors have conducted a thorough examination of the pertinent matters concerning the privacy and security aspects of the Electronic Health Record (EHR) system, as documented in the academic literature available to the public. This study was carried out by using a comparative framework derived from the ISO 27799 standard. Existing literature has shown that Electronic Health Record (EHR) solutions obtained from different vendors often have pre-established security and privacy features. To address the current topic, a thorough analysis of the actual EHR systems in use is necessary [56-58]. Furthermore, the authors have a firm conviction that by emphasizing and examining the privacy and security suggestions presented in the available academic literature, they might potentially serve as a substitute for the actual ideas for EHR privacy and security [59-62].

Issues Regarding the Confidentiality and Protection of Electronic Health Records

Multiple polls have consistently highlighted many issues surrounding the confidentiality of health information. According to Win [63], over 66% of consumers showed concern for the privacy of their personal health information, while just 39% of respondents believed that their health data were adequately protected and secure. According to the study, a significant number of respondents expressed both a lack of concern about the security of their data and a lack of trust in its safety [45]. Perera et al. [52] conducted a survey in which 50% of the participants expressed concern about the security of their data due to its transmission via the internet. Approximately 50% of the research participants in a study done by Ancker et al. [7] held the belief that sharing their health information may have a negative impact on their privacy regarding health information. Several research examining individual concerns about information privacy have shown that these issues are crucial for the effective use of electronic health records systems.

The privacy and security concerns of the Internet of Things arise from the distinctive characteristics of IoT networks, which set them apart in several ways. The qualities include heterogeneity, an uncontrolled environment, limited resources, and a strong need for scalability. Even the tiniest processor architectures already include a highly efficient cryptographic engine and enough program memory to execute essential security activities. Lafky & Horan [45] suggest that security needs for Internet of Things (IoT) systems may be categorized based on their distinct characteristics. These requirements can be grouped into the following settings: identity management, network security, resilience and trust, and privacy. In this example, the authors focus on several designs that have been extensively suggested for the internet of things in the academic community. They analyze if these architectures fulfill the necessary security measures. The critical analysis reveals that although several security demands are taken into account, none of the designs fully address all of these criteria [45].

The trust and privacy standards are the most neglected. The existence of computers necessitates the existence of a widely accepted model for information technology security, commonly referred to as CIA. This model emphasizes three crucial security features: confidentiality, which aims to prevent unauthorized access to data; integrity, which ensures that data remains unaltered; and availability, which guarantees that data can be accessed whenever necessary [45].

The three characteristics have been thoroughly explained and arranged in the shape of a triangle, with each property positioned at one of the vertices. Over the years, the model has undergone several modifications, but the core qualities, known as CIA, have stayed constant. An aspect that has not been extensively emphasized is that these three traits cannot be completely realized simultaneously, since they are thought to be mutually incompatible. Given a fixed allocation of resources, it is impossible to enhance the overall availability without sacrificing the accuracy, secrecy, or both. Traditional security measures for general information-processing computer systems have primarily prioritized the confidentiality of the data. However, in the case of embedded systems and the Internet of Things (IoT), it can be argued that the other two aspects, namely integrity and availability, are even more critical than they are in office information systems [38]. Another significant discovery is that the variation in the method I typically affects the collaboration between conventional IT systems and control system managers.

Whetstone & Goldsmith [61] validated that an individual's trust in the privacy and security of their medical information positively impacted their motivation to use an electronic health record. Bansal et al. [11] verified that privacy concerns had a detrimental effect on individuals' willingness to disclose their health information over the internet. Anderson & Agarwal [8] did a study that found a detrimental impact of worries about health information privacy on people' willingness to cooperate in granting access to their personal health information.

However, Dinev et al. [22] discovered that there is a weak correlation between individuals' worries about the privacy of their health information and their attitude towards electronic health records. Angst & Agarwal [9] reached the same conclusion about the acceptability of electronic health records. A research done by Ermakova et al. [25] shown that patient' worries about health information privacy had a negative impact on their readiness to enable health care professionals to share their medical data while using cloud computing technology. In the context of healthcare, trust becomes more crucial than discounts due to the presence of privacy issues, even in the case of secondary usage. In a study conducted by Kuo et al. [44], it was found that there are valid concerns about the privacy of health information. These concerns manifest in various ways, such as patients refusing to provide their personal information to healthcare providers, providing false personal information to medical facilities, requesting the removal of their personal information, making negative comments about their experiences to friends, filing complaints directly with medical facilities, and filing complaints indirectly with third-party organizations.

Rohm and Milne [54] found that customers' level of worry is higher when an organization obtains a list that includes individual medical history, as opposed to a list that just has broad information. Zulman et al. [64] conducted a research that found that people have different preferences when it comes to sharing their electronic health information, depending on the kind of information being shared. King et al. [40] have observed that privacy concerns differ for certain components of health data. The health institution has proven that the topics of most concern to individuals are infertility, abortion, and sexually transmitted illnesses, since they directly impact their families. Individuals exhibited diminished privacy apprehensions about some details in their health records, including religion, date of birth, blood group, language, gender, blood pressure status, and cancer status.

Current Electronic Health Record (EHR) Systems Include Advanced Security and Privacy Measures

The study of many research studies has included three key security-safeguard themes: physical, technological, and administrative. These topics include several security measures used by healthcare administrations to enhance the protection of sensitive health information stored in electronic health records. The subject of administrative safeguard is the primary safeguard that includes strategies such as conducting audits, appointing an information security officer, and developing contingency plans [62]. This topic incorporates protections that prioritize the implementation of security processes and policies in accordance with regulatory requirements. The second topic pertains to physical safeguards, including the strategies mentioned in organizational safeguards. Furthermore, it emphasizes the protection of health information in a physical sense, ensuring that unauthorized individuals or potential abusers are unable to access the software or hardware [62]. The breach of physical protections is the second most ranking cause of security breaches, accounting for 47% of all incidents. One example of a strategy used in physical safeguards is the implementation of assigned security responsibilities [46].

Technical safeguards, the third group of topics, provide comprehensive security for the information system inside a health organization's network. This issue is crucial for maintaining the security of the company since most security breaches occur via electronic media, such as PCs and other portable electronic devices [47]. This subject incorporates security measures such as the use of firewalls and encryption, virus scanning, and authentication protocols [46]. Nevertheless, Lemke [46] determined that firewalls and encryption were the most often used security solutions. Additional noteworthy security measures that are often used include antivirus software, chief information security officers, and cloud computing. However, the deployment of these measures is contingent upon the available money [27].

According to Liu et al. [47], their study revealed that physical precautions, such as physical access control, are used to avoid theft. These safeguards include the installation of locks on computers. Additionally, technological safeguards, such as firewalls and encryption, are implemented to prevent electronic breaches. Amer [6] conducted a research on informatics by ethically using genetic information and electronic health data. He recognized that encryption may provide a technological means of protection, while administrative measures used a security method of de-identifying gathered samples or research data. Firewalls, encryption, decryption, extensive education and security strategies, and engaging a Chief Information Security Officer are all examples of technical and administrative protections that may be used to protect against security threats [37]. According to Wikina [34], administrative safeties include a manager's approval for releasing paper data including patient information and conducting trainings on how to handle missing documents. Physical protections entail the installation of security cameras.

With the continuous advancements in contemporary technology, healthcare businesses are increasingly becoming targets for security breaches. Firefox is used as a technique to safeguard the information technology systems of healthcare companies [18, 19]. Firefox is very successful in enhancing network security inside an enterprise and safeguarding the confidentiality of health information on the network. Firefox is used for safeguarding the firm from potential dangers that may disrupt its information network, both inside and outside. They appear in numerous forms [47].

The use of level gateway represents the third classification of firewalls. They serve as gatekeepers for the organization's network by scanning the IP web page for any risks before allowing it to be accessed by end users. The status inspection firewalls allow access to their external network connections via the gateway, therefore preventing the entrance of external networks into the organization's intranet [47]. Submission equal gates effectively safeguard electronic health data by preventing hackers from directly into the system and accessing the protected health information. Implementing this set of firewalls can be challenging for organizations due to their intricate nature and substantial associated expenses.

Consequently, it is imperative to conduct comprehensive evaluations of both external and internal factors within the organization to determine the feasibility and suitability of deploying the firewall for each organization. Ultimately, we own a collection of firewalls often known as the network address translator. It helps in concealing the intranet IP addresses of the company to prevent external users with malicious intentions from accessing them and causing harms [47]. A network address translator creates a barrier between an organization's intranet and the local area networks. While firewalls are very efficient in protecting the security of electronic health data, it is crucial to implement all four elements of its protection techniques. The sequence of phases comprises service control, direction control, user control, and behavior control [62]. Prior to implementing any kind of firewall, it is crucial for the business to do a comprehensive requirements assessment, financial evaluation, and assessments of both external and internal risks. If an organization fails to conduct the aforementioned evaluations or does not complete the four security plans, it may have a detrimental impact on the security of patients' electronic health data or potentially the whole information system of the company [18, 19].

Cryptography has been used as a means of safeguarding and preserving the integrity of electronic health records. Encryption has enhanced the security of electronic health records while transferring health information. The communication of health information must adhere to particular standards, which often include organizations documenting the exchange method when encryption is either activated or off [60]. HIPAA included measures to use encryption for safeguarding health information [20].

Mobile agents are used to enhance the accessibility and security of electronic health records while transmitting patient data across facilities [46]. Utilizing usernames is an additional method of employing encryption. They may assist in avoiding security breaches by incorporating individual privacy into passwords and promoting regular password changes among users. To minimize the risk of password guessing by hackers, it is important to avoid using widely used names and dates as passwords. Implementing username and password security measures is beneficial for establishing effective controls. The role-based controls limit data access to users by implementing usernames and passwords generated by system administrators. This method fails to provide adequate safeguarding of information inside electronic health records against internal attacks. Employees must log out of the system after they have finished in order to protect sensitive health information from being accessed by unauthorized individuals [46].

Conclusion

The current study has conducted a comprehensive examination of existing literature pertaining to the security and privacy of electronic health record systems. The study has examined several security and privacy concerns that emerge from the use of Electronic Health Records (EHRs) and explores viable remedies. The research clearly demonstrates that Electronic Health Records facilitate the seamless sharing of structured medical data across authorized healthcare providers, hence enhancing the overall quality of healthcare services provided to patients. Utilizing e-health expands consumers' cognitive capacity and facilitates efficient networking among healthcare professionals.

Electronic health records provide seamless sharing of medical information across stakeholders, enabling easy access and updating of patient information throughout the course of treatment. Security and privacy considerations are crucial in such systems, since the patient might encounter significant issues if sensitive information is revealed to a third party. Based on the studied publications and analysis of security areas, it is clear that many policies and standards pertaining to privacy and security are used in electronic health records. Nevertheless, it is important to synchronize these systems in order to address any conflicts and discrepancies across standards. Several encryption techniques have been suggested by different publications.

It is strongly advised to implement an effective encryption method on the current electronic health records (EHR) that can be conveniently used by healthcare professionals and patients. The most favored access control paradigm in electronic health record systems is Role-Based Access Control (RBAC), whereas the most effective authentication techniques are passwords/logins and digital signatures. Efficiently overseeing an electronic health record necessitates a multidisciplinary team of experts in communications, instrumentation, and computer science. This team is responsible for facilitating the seamless flow of medical data over vast geographic areas.

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. 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.
6. 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.
7. Amer K. Informatics: ethical use of genomic information and electronic medical records, J Am Nurses Assoc 2015;20(2).
8. 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.
9. 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.

10. 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.
11. Bahtiyar S,, Çagˇlayan 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.
12. 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.
13. 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.
14. Brumen B, Hericˇko M, Sevcˇnikar 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.
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.
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. 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.
35. Hussain M et al. A security framework for mHealth apps on Android platform. Comput Secur 2018;75:191–217.
36. 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.
37. Ives TE. The New 'E-Clinician' guide to compliance. Audiol. Today. 2014;26 (1):52–3. [Google Scholar]
38. 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.
39. 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.
40. Kiah MLM et al. MIRASS: medical informatics research activity support system using information mashup network. J Med Syst 2014;38(4):37.
41. 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.
42. 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.

43. 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.
44. Kruse CS, Smith B, Vanderlinden H, Nealand A. Security techniques for the electronic health records. J Med Syst 2017;41(8):127.
45. 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.
46. 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.
47. Lemke J. Storage and security of personal health information. OOHNA J 2013;32(1):25–6.
48. 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
49. Ma Q, Schmidt MB, Pearson JM, Herberger GR. An integrated framework for information security management. Rev Bus 2009;30(1):58–69.
50. 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.
51. 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.
52. 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]
53. 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.
54. 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.
55. 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.
56. Rothstein MA. Health privacy in the electronic age. J Leg Med 2007;28 (4):487–501.
57. 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.
58. 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.
59. 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.
60. 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.

61. 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.
62. Whetstone M, Goldsmith R. Factors influencing intention to use personal health records. Int J Pharmaceutical Healthcare Marketing 2009;3(1):8–25.
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.