JMSCR Vol||11||Issue||06||Page 88-93||June 2023

http://jmscr.igmpublication.org/home/
ISSN (e)-2347-176x ISSN (p) 2455-0450
crossref DOI: https://dx.doi.org/10.18535/jmscr/v11i6.17

IGM Publication
Journal Of Medical Science And Clinical Research
An Official Publication Of IGM Publication

Security & Privacy of Electronic Health Records

Authors
Sultan O. Aladwani[1], Mohammed A. Almotairi[2]
[1,2]Specialist-Health Administration

Abstract
Healthcare facilities like hospitals and clinics are adopting new technology at a dizzying pace. However, confidentiality concerns are frequently neglected, placing healthcare institutions at risk of cyber security problems, fines, reputational harm, and even catastrophic patient implications. Clinical documentation, patient profiles, lab findings, imaging findings, and diagnostic procedures make up Electronic Health Record (EHR) systems. EHRs are getting more and more complex with time, necessitating more and more data storage. In order to secure healthcare-based technologies and networks, new protection and security techniques are being explored with the growth of the IoT, Software as a service, and City Development platforms.

Introduction

A healthcare provider's long-term digital storage of a physician's physiological history is known as an electronic health record. It consists of all the crucial organizational medical studies necessary to understand a person's treatment from a specific service, such as population demographics, medication interactions, alarming symptoms, medical histories, inoculation records, lab tests, and test results. The majority of healthcare facilities and organizations keep records of healthcare in print, which results in a sizable complete document. As a result, most companies are interested in switching from paper-based to EHR systems. (Paris-Rocquencourt et al., 2010)

Evidence-based medicine is promoted, expenses are reduced, care is provided with higher quality, unified healthcare information helps with record keeping, and portability of the information is ensured. In order to function properly, electronic medical records should follow security laws, obtain comprehensive data, be instantly flexible, and be resistant to failure. However, there have been a number of issues that have prevented the use of patient data. They include attitude, a few organizational characteristics, and funding for innovation.

Electronic medical records (EMRs), also known as health records (EHRs), are becoming more and more common in the context of e-health. Digital medical records, which are regarded as a key element in the application of e-health, include individual health-related data. Legal documents created in hospital settings constitute an electronic medical record. The principal source of information for an electronic health care record would then be this information. (Achampong, 2013)

Healthcare personnel do not entirely trust the electronic medical records system, despite the fact that hospitals use it in their daily operations. According to Albahri, the word "e-health" first appeared at the beginning of the twenty-first century and refers to the use of contemporary information and communication technology to deliver medical services in the healthcare industry. (Albahri et al., 2018)

Managing electronic health requires a multi-disciplinary staff that includes experts in telecom, sensors, and computational science to enable the transmission of medical data over wider localities. Muzammil Hussaina and colleagues (2015) The use of e-health encourages effective networking among medical experts and allows consumers to think more broadly. 2014's (Kiah et al.) Two benefits of enhancing the healthcare system are the efficiency of patient safety and the calibre of medical care delivered.

Transparency, privacy, and anonymity are major concerns that must be resolved in electronic medical records systems. (Alanazi et al., 2014)

Despite their close relationship, privacy and confidentiality are actually rather distinct. While security is characterised as the level during which access to someone's personal information is confined and allowed for those who are authorised only, privacy refers to the freedom that a person has to decide on their own when, how, and the extent to which personal data is given or communicated by others.(Sittig & Singh, 1970)

When sensitive information is transferred or shared without authorization, a data breach may result.

Invasions of privacy may also result from the systemic identification that is unavoidably found throughout the entire computerised healthcare system, as well as from centralize technologies and entities that keep an eye on both healthcare physicians and patients (Sittig & Singh, 1970). The healthcare provider may, however, unintentionally or on purpose, misuse the medical record entries in situations when the present administration, businesses, drug makers, investigators, and scientists may have justification to access the client's health documents in order to get certain information.

The three fundamental needs for information systems security, according to Dehling and Sunyaev (Dehling & Sunyaev, 2014), are security, validity, and accessibility. Confidentiality is the ability to limit the availability of data to those who are not allowed to see it while it is being transmitted, stored, or processed. By using technology tools like data encryption or restricting access to the systems, confidentiality can be established. Concentrating on morality like maintaining professional quiet is another way to attain privacy. But (Dehling & Sunyaev, 2014) observed that while encryption is frequently used for health records delivered over wireless connections, it is less frequently employed for data saved on portable apps and other memory sticks.

Due to the extremely sensitive information on patients and patients that they hold, the requirement for anonymity is a solution to personal information, which is also very crucial in the healthcare business. The term "accessibility" refers to a variety of concepts, including scalability, durability, and the capacity to restore lost data.

Health workers do not entirely trust the electronic medical record platform, despite the fact that clinics use it in their daily operations. The use of e-health encourages effective communication between medical experts and allows people to think more widely. Enhancing healthcare has advantages including enhancing the effectiveness of healthcare organisations and enhancing the standard of services for patients. (Dehling & Sunyaev, 2014)

Transparency, security, and authenticity are major concerns that must be considered in electronic systems for medical records. Despite their close relationship, privacy and confidentiality are actually rather different. While protection is described as the level during which obtaining a woman's personally identifiable information is

limited and permitted for those who are authorized only, confidentiality refers to the privilege that someone has to decide on their own when, how, and the extent to which individual data is disclosed or communicated by others.

Concerns on Privacy and Security of Electronic Health Records

The network of objects' worries regarding confidentiality and safety start with the connections' fundamental qualities, which make them different in their own ways. These characteristics include diversity, a volatile climate, a shortage of resources, and a greater requirement for flexibility. Currently, extremely nice crypto engines and enough memory bandwidth are available on even the tiniest CPU platforms to accomplish necessary security functionalities. (Whetstone & Goldsmith, 2009)

In fact, all of these traits have been clearly articulated in the form of a triangle with the attributes at the sides. The fundamental one, the CIA, hasn't changed over time, but the paradigm has evolved to encompass a variety of other important traits. There hasn't been much discussion of the idea that these three qualities cannot be fully reached concurrently since they are believed to be inherently incompatible. Assuming the same quantity of resources, it is difficult to improve the accessibility overall without compromising correctness, confidentiality, or maybe both. (Jing et al., 2014)

It has been proven that among the health centre's services, individuals are more concerned about concerns relating to infertility, abortion, and sexually transmitted illnesses, among others that have a direct impact on their families. Some of the information in health records that people expressed significantly less privacy worry over were their profession, year of birth, genetic makeup, language proficiency, gender, hypertension status, and malignancy status.

Security and Privacy Features of current EHR systems

The major security-safeguard issues of mechanical, financial, and administrative security have been utilised in the study of various studies. In order to increase the confidentiality of the confidential medical data contained in electronic health records, healthcare providers use a number of security approaches. A first precautionary relates to administrative safeguard, which covers important techniques including doing audits, employing a supervisor accountable for information security, and creating contingency plan (Wikina, 2014). Support systems in this area stress adherence to security norms and procedures. The subject, "Hardware Safeguards," focuses on physically securing the healthcare information in order to prevent access by unauthorized persons or those who would misuse it. It involves the following precautions measures mentioned before. As modern science advances further, health institutions are increasingly being attacked for data breaches. Institutions, including the Diagnostic Engineering I.T. Town, the American College of Diagnostic Designing, and the Universal health care Tracking and Management Systems Society, among others, have taken risk management very seriously and recognize how crucial it is to keep up with new technology and dangers (Wikina, 2014). Together with the designated organisations, the previously mentioned risk evaluation and control stages make sure that the healthcare organisation is advanced in protecting patient information in electronic healthcare records.

The third class of firewalls is used as a level gateway. Whenever the IP web address is examined for dangers before being passed to end users, they serve as the organisation's gatekeepers for the network. The gate provides access to the status inspection firewalls' external communication networks, preventing the network from entering the organisation's intranet. Electronic health records have been successfully safeguarded by submission identical gates because

they stop attackers from immediately logging into the system and gaining access to the private health data. (Vincent Liu, 2015)

Digital health records have been secured or protected using cryptography. When transferring health information, electronic medical records are now more secure thanks to the use of cryptography. The process of transferring health information contains guidelines that must be adhered to, and in most cases, requires companies to document the exchange procedure whether encryption is set or off.

As a consequence of the expanding utilisation technology, a thorough research of cloud computing for integration with Electronic health records has been conducted. Thanks to the framework that public cloud provides, one can carry out digital projects, knowledge exchange, and the "having to rent" of space and computer power. Healthcare organisations are in a position to build an Electronic health record for less money while also implementing cryptographic procedures by moving ownership or lowering maintenance expenses in this way. Regardless how appealing the cloud computing platform may seem, anti-virus software is a more popular safety mechanism.

Information technology security incidents in healthcare settings

The use of technologies of information and communication (ICT) has helped patients move from their stereotypical families as passive receivers of healthcare services to more engaged roles that involve understanding their health records, making decisions, and participating in the decision-making process. The difficulty of determining the degree of flexibility that should be given to issuers and covered entities has grown as a result. By integrating security and confidentiality with accountability and key distribution in electronic health records technologies, there are a variety of solutions to some of the problems that have been found. Recent years have seen a rise in privacy and security issues around the use of electronic medical records. (Arnab Ray et al., 2021)

Conclusion

Participants may easily interchange medical information thanks to digital health records, which also make it easy to examine and modify patient data as a person gets care. But in such platforms, privacy and security concerns are crucial since it's feasible that the individual could have serious troubles if crucial data is made available to a third - party provider. It is abundantly clear from the publications examined and the security technology examined that various privacy and stability laws and procedures pertain to digital health records.. But in order to address any contradictions and misunderstandings in the law, these systems must be integrated. Different encryption approaches have been developed by studies done.. (Dorgham et al., 2018)

Regarding the most recent EHR data, it is actually recommended that an effective cryptography technique be used that is consumer for both physicians and patients. The best control mechanism for computerized health care systems is RBAC, while the best electronic certificates are user and passwords and cryptographic algorithms. Successfully managing an electronic health-care record necessitates a team approach that comprises communication, instruments, and programming skills in order to ease the exchange of medical information across greater geographic locations.

References

1. A. links open overlay panel Arnab Ray, Arnab Ray, and Abstract The purpose of this chapter is twofold. First, “Basic cyber security concepts,” *Cyber security for Connected Medical Devices*, 12-Nov-2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/B9780128182628000085. [Accessed: 07-Jan-2023].

2. Author links open overlay panel Muzammil Hussaina Ahmed Al-Haiqia O.A. Zaidanab Person Envelope B.B. Zaidana M.L.M. Kiaha Nor Badrul Anuara Mohamed Abdulnabia, Muzammil Hussain, a, Ahmed Al-Haiqia, A.A. Zaidanab Person Envelope, b, B.B. Zaidana, M.L.M. Kiaha, N. Badrul Anuar, Mohamed Abdulnabi al, Highlights• Mapping the research landscape of smartphone medical apps into a coherent taxonomy.•Figure out the motivation of using smartphone apps in medicine & healthcare.•Highlight the open challenges that hinder the utility of medical apps.• Recommendation, and Abstract Objective T o survey researchers' efforts in response to the new and disruptive technology of smartphone medical apps, "The landscape of research on smartphone medical apps: Coherent taxonomy, motivations, open challenges and recommendations," Computer *Methods and Programs in Biomedicine*, 03-Sep-2015. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0169260715002254. [Accessed: 07-Jan-2023].
3. D. F. Sittig and H. Singh, "A new socio-technical model for studying health information technology in complex Adaptive Healthcare Systems," *Springer Link*, 01-Jan-1970. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-17272-9_4. [Accessed: 07-Jan-2023].
4. H. O. Alanazi, A. A. Zaidan, B. B. Zaidan, M. L. M. Kiah, and S. H. Al-Bakri, "Meeting the security requirements of electronic medical records in the era of high-speed computing - journal of medical systems," *Springer Link*, 07-Dec-2014. [Online]. Available: https://link.springer.com/article/10.1007/s10916-014-0165-3. [Accessed: 07-Jan-2023].
5. M. D. Vincent Liu, "Data breaches of Protected Health Information," *JAMA*, 14-Apr-2015. [Online]. Available: https://jamanetwork.com/journals/jama/article-abstract/2247135. [Accessed: 07-Jan-2023].
6. M. L. M. Kiah, B. B. Zaidan, A. A. Zaidan, M. Nabi, and R. Ibraheem, "MIRASS: Medical Informatics Research Activity Support System USING INFORMATION MASHUP Network - Journal of Medical Systems," *Springer Link*, 04-Apr-2014. [Online]. Available: https://link.springer.com/article/10.1007/s10916-014-0037-x. [Accessed: 07-Jan-2023].
7. M. Whetstone and R. Goldsmith, "Factors influencing intention to use personal health records," *International Journal of Pharmaceutical and Healthcare Marketing*, 03-Apr-2009. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/17506120910948485/full/html. [Accessed: 07-Jan-2023].
8. O. Dorgham, B. Al-Rahamneh, A. Almomani, M. Al-Hadidi, and K. F. Khatatneh, "Enhancing the security of exchanging and storing DICOM medical images on the cloud," *International Journal of Cloud Applications and Computing (IJCAC)*, 01-Jan-2018. [Online]. Available: https://www.igi-global.com/article/enhancing-the-security-of-exchanging-and-storing-dicom-medical-images-on-the-cloud/196196. [Accessed: 07-Jan-2023].
9. Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: Perspectives and challenges - wireless networks," *SpringerLink*, 17-Jun-2014. [Online]. Available: https://link.springer.com/article/10.1007/s1

1276-014-0761-7. [Accessed: 07-Jan-2023].

10. S. B. Wikina, "What caused the breach? an examination of use of information technology and health data breaches," *Perspectives in health information management*, 01-Oct-2014. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4272442/. [Accessed: 07-Jan-2023].
11. T. Dehling and A. Sunyaev, "Secure provision of patient-centred health information technology services in public networks-leveraging security and privacy features provided by the German nationwide health information technology infrastructure - electronic markets," *SpringerLink*, 08-Feb-2014. [Online]. Available: https://link.springer.com/article/10.1007/s12525-013-0150-6. [Accessed: 07-Jan-2023].
12. E. K. Achampong, "Electronic health record (EHR) and cloud security: The current issues," *UCC IR Home*, 01-Dec-2013. [Online]. Available: https://ir.ucc.edu.gh/xmlui/handle/123456789/5272. [Accessed: 07-Jan-2023].
13. O. S. Albahri, A. S. Albahri, K. I. Mohammed, A. A. Zaidan, B. B. Zaidan, M. Hashim, and O. H. Salman, "Systematic review of real-time remote health monitoring system in triage and priority-based sensor technology: Taxonomy, open challenges, motivation and recommendations - Journal of Medical Systems," *SpringerLink*, 22-Mar-2018. [Online]. Available: https://link.springer.com/article/10.1007/s10916-018-0943-4?utm_source=getftr&utm_medium=getftr&utm_campaign=getftr_pilot. [Accessed: 07-Jan-2023].
14. T. A. I. N. R. I. A. Paris-Rocquencourt, T. Allard, I. N. R. I. A. Paris-Rocquencourt, N. A. I. N. R. I. A. Paris-Rocquencourt, N. Anciaux, L. B. I. N. R. I. A. Paris-Rocquencourt, L. Bouganim, Y. G. I. N. R. I. A. Paris-Rocquencourt, Y. Guo, L. L. F. I. N. R. I. A. Paris-Rocquencourt, L. L. Folgoc, B. N. I. N. R. I. A. Paris-Rocquencourt, B. Nguyen, P. P. I. N. R. I. A. Paris-Rocquencourt, P. Pucheral, I. R. C. S. University, I. Ray, C. S. University, I. R. C. S. University, I. Ray, S. Y. I. N. R. I. A. Paris-Rocquencourt, S. Yin, and O. M. V. A. Metrics, "Secure Personal Data Servers: A Vision Paper: Proceedings of the VLDB endowment: Vol 3, no 1-2," *Proceedings of the VLDB Endowment*, 01-Sep-2010. [Online]. Available: https://dl.acm.org/doi/10.14778/1920841.1920850. [Accessed: 07-Jan-2023].