OPEN ACCESS

Saudi Journal of Medicine

Abbreviated Key Title: Saudi J Med
ISSN 2518-3389 (Print) | ISSN 2518-3397 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

Enhancing the Security of Medical Records in the Age of Cyber Threats: A Comprehensive Approach

Sultan Abdullah Almohesen[1*], Ahmad Abdulrahman Alnoweser[2], Nasser Suliman al- Nasser[3], Sulaiman Al Bawardi[4], Ibrahim S ALFwzan[5]

[1-5]Health Information Techian, Health Affairs at the Ministry of National Guard

DOI: https://doi.org/10.36348/sjm.2024.v09i12.006 | **Received:** 17.11.2024 | **Accepted:** 23.12.2024 | **Published:** 24.12.2024

***Corresponding Author:** Sultan Abdullah Almohesen
Health Information Techian, Health Affairs at the Ministry of National Guard

Abstract

The increasing digitization of medical records and the concurrent rise in cyber threats pose significant challenges to the security and integrity of health data globally. This article reviews contemporary challenges and solutions for enhancing the protection of medical records against potential cyber-attacks and inadvertent breaches. It addresses the current vulnerabilities that exist within systems handling medical records, outlines advanced technological solutions such as encryption, blockchain, AI, and multi-factor authentication, and discusses comprehensive policy measures that include regular audits, privacy by design concepts, and training programs. The article also explores critical legal and ethical considerations, emphasizing the need to balance accessibility and privacy. Finally, it proposes long-term strategic approaches to foster innovation in healthcare cybersecurity. Through this comprehensive review, the article aims to delineate effective strategies for securing medical records in the age of cyber threats, contributing to the safeguarding of patient privacy and the trust integrity of healthcare systems.

Keywords: Cybersecurity, Medical Records, Data Privacy, HIPAA/GDPR, EHRs (Electronic Health Records).

INTRODUCTION

In the era of digital health information, the security of medical records has become paramount. As healthcare providers increasingly adopt digital systems, such as Electronic Health Records (EHRs), substantial benefits have emerged, including improved efficiency and continuity of care (Jawad, 2024). However, the shift from paper-based to digital systems has introduced significant vulnerabilities that cybercriminals can exploit (Alarfaj & Rahman, 2024). A study by Tertulino *et al.*, 2023, shows the source of the U.S. information reveals that over two million people with mental health illnesses never receive medical care because of privacy issues. Keshta and Odeh's (2021) research reveals that patients with an infection or infertility background avoid disclosing their medical records and medical history, which makes matters worse. Thus, they refuse medical support for fear of their data being digitally stored.

The repercussions of compromised health data are profound, affecting patient privacy, public trust in healthcare systems, and compliance with legal standards like the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). Consequently, understanding and implementing robust cybersecurity measures is crucial in the current landscape where cyber threats are becoming more sophisticated (Shaygan and Daim, 2021).

This article delves into the multifaceted approach required to enhance the security of medical records amidst escalating cyber threats. It begins by examining the current landscape of vulnerabilities in systems handling digitized medical records. It then explores various technological innovations, such as blockchain and artificial intelligence (AI), that can play pivotal roles in safeguarding these records. Alongside technological solutions, the article evaluates essential policy measures, including legal frameworks and institutional policies that govern the access and handling of sensitive medical data. Ethical considerations are also discussed, focusing on the necessity of balancing patient privacy with the benefits of greater accessibility to health data.Moreover, the article proposes a strategic outlook for the long-term, emphasizing the need for ongoing innovation in security technologies and collaboration among stakeholders in the healthcare sector. This comprehensive approach ensures that advancements in healthcare cyber security keep pace with ever-evolving threats, thus protecting individuals' sensitive health information against unauthorized access and ensuring a resilient healthcare system.

METHODOLOGY

The research reviewed the systematic literature review to gather data from previous studies, academic papers, technology reports, and regulations related to the security of medical records. Sources included peer-reviewed journals, conferences, and updates on technological advancements. This review helped map out the existing body of knowledge and identify gaps in technology, policy enforcement, and compliance with legal frameworks.

LITERATURE REVIEW

1. The Current Landscape of Medical Record Vulnerabilities

Medical records, traditionally a trove of personal health information, have increasingly become digitized in the form of Electronic Health Records (EHRs) (Hall, 2009). The advantages of EHRs include enhanced continuity of care, reduced medical errors, and overall improved efficacy within healthcare systems. However, digitization brings significant vulnerabilities (Wijayanti *et al*., 2024). Healthcare data breaches are often due to cyber-attacks such as phishing, malware, and ransomware or due to human errors including improper disposal of records, lost/stolen devices, and inadvertent disclosures (Wijayanti *et al*., 2024). Various studies, such as those by Shaygan and Daim (2021), highlight that the healthcare industry remains particularly susceptible to ransomware attacks, data breaches, and other cyber threats due to outdated infrastructure and insufficient cybersecurity measures.HIPAA (Health Insurance Portability and Accountability Act) in the U.S., GDPR (General Data Protection Regulation) in the EU, and similar regulations worldwide set forth stringent mandates regarding the handling and protection of patient data, but adherence is uneven, and enforcement can be challenging (Kruse *et al*., 2017).

2. Advanced Technological Solutions

2.1. Encryption

Encryption should be at the foundation of any strategy to secure medical records. Data encryption should occur both at rest and during transmission, making sensitive information unreadable without the appropriate decryption keys (Hazra *et al*., 2024) .Advanced encryption standards, like AES-256, provide robust security against brute-force attacks(Hazra *et al*., 2024). Kruse *et al*., (2017) offer numerous techniques for bolstering EHRs' security, such as implementing stronger data encryption standards, regular security audits, and employee training programs, which are crucial for maintaining a secure operational environment. Also, Williams and Woodward (2015) underscore the particular vulnerabilities of medical devices to cyber-attacks, which compound the complexity of securing medical records.

Encryption is a fundamental pillar for protecting data integrity and confidentiality in healthcare systems. By converting information into a coded format that is unreadable without a specific decryption key, encryption ensures that data intercepted during transmission remains secure from unauthorized access (Chen *et al*., 2019). Research by Kruse *et al*., (2017) emphasizes the critical role of encryption in securing patient data stored in EHRs, especially when transmitted over public networks.

2.2. Blockchain Technology

The decentralized nature of blockchain technology is valuable for the secure sharing of medical records across disparate entities in the healthcare ecosystem. By creating an immutable ledger of patient data, blockchain can enhance transparency while maintaining confidentiality, as access and edits are securely logged and visible (Sabry *et al*., 2019).

In recent years, the blockchain technology garnered significant attention from both the industrial and theoretical fields (Khezr *et al*., 2019) because of its potential to address security, storage, and data transmission issues. However, this new technology has a direct effect on the business process of healthcare outcomes for organizations and external collaborators, as well as on patients' health services, data management, improvement of compliance, and the efficient use of healthcare data flow (Mackey *et al*., 2019).

2.4. Multi-Factor Authentication (MFA)

Implementing MFA for accessing medical records systems can significantly reduce the risk of unauthorized access. This method uses two or more verification factors to ensure that the person requesting access is legitimate, thereby providing a robust barrier against intrusion (Finlayson *et al*., 2019).

Multi-factor authentication adds an additional layer of security by requiring more than one method of authentication from independent categories of credentials. This method significantly lowers the risk of unauthorized access because the likelihood of an attacker obtaining two or more separate authentication factors is minimal. Alarfaj & Rahman (2024) advocate for widespread adoption of MFA in healthcare settings to enhance security for accessing EHR systems. Moreover, Wijayanti *et al*., (2024) suggest that combining MFA with robust security policies creates a strong deterrent against unauthorized data access.

3. Comprehensive Policy Measures

3.1. Regular Audits and Compliance Checks

Healthcare organizations must commit to regular audits of their security practices and privacy compliance. These audits help identify vulnerabilities before they can be exploited and ensure practices align with both internal policies and external regulatory requirements (Greenfield *et al*., 2011).

The necessity of regular audits and compliance checks in the healthcare sector cannot be overstated. Jawad's (2024) research underscores the importance of continual assessment and monitoring to detect and mitigate potential security threats and privacy breaches. Regular audits help in identifying vulnerabilities in digital healthcare systems and ensure compliance with health information privacy standards. Alarfaj and Rahman (2024) add that risk assessment using a risk matrix can guide the auditing processes, helping healthcare organizations prioritize risks and allocate resources effectively to address the most critical vulnerabilities first.

3.2. Privacy by Design

Integrating privacy into the system design and business practices is crucial. This approach ensures that privacy considerations are not afterthoughts but integral to system architecture, thereby potentially preventing breaches before systems are even deployed.

The concept of 'Privacy by Design' is a proactive approach to embedding privacy into the design and architecture of IT systems and business practices. Tertulino *et al*., (2023) discuss how privacy by design can be implemented in electronic health records to ensure privacy considerations are integrated from the outset, rather than being added as an afterthought. This approach not only helps in complying with legal requirements but also enhances trust with patients who are increasingly concerned about the privacy and security of their personal health data.

3.3. Training and Awareness Programs

Human error remains one of the largest threats to the security of medical records. Regular training and ongoing awareness programs for healthcare staff about phishing tactics, proper data handling procedures, and security best practices are essential to cultivating a security-conscious culture (Hakimi *et al*., 2024).

Training and awareness programs are critical in equipping healthcare professionals and IT staff with the knowledge and skills needed to protect digital healthcare systems. As Keshta and Odeh (2021) point out, human error remains one of the largest threats to information security. Comprehensive training programs that are updated regularly can mitigate this risk by ensuring that all personnel are aware of the latest threats and know how to follow best security practices.

4. Legal and Ethical Considerations

Maintaining the balance between accessibility and privacy is a legal and ethical challenge. Legislations must evolve with technological advancements to protect sensitive information without impeding healthcare delivery. Ethically, the principle of minimum necessary use should always be applied, ensuring that the exposure of patient data is minimal and only as broad as necessary for healthcare purposes.

Navigating the legal and ethical aspects of digital healthcare systems is complex. The confidentiality of patient data is not just a technical issue but also a legal requirement. Kruse *et al*., (2017) emphasize that adherence to laws such as HIPAA in the United States, GDPR in Europe, and other national and international regulations is essential. These laws provide a framework for protecting personal data and offer a guideline for what organizations must do to comply. Williams and Woodward (2015) further discuss the ethical implications, including the ethical use of medical devices and the need for transparency in how patient data is used and shared.

5. Long-Term Strategic Approaches

Long-term strategies might include fostering collaborations between the public and private sectors to nurture innovation in cybersecurity solutions specifically tailored for healthcare. Additionally, international cooperation can help standardize regulations and facilitate a more robust exchange of threat intelligence.

Long-term strategic approaches involve looking beyond immediate technological fixes and developing comprehensive strategies that encompass technology, people, and processes. Shaygan and Daim (2021) describe a technology management maturity assessment model that can be used by healthcare organizations to evaluate their current technologies and processes and identify areas for improvement. Wijayanti *et al*., (2024) suggest that focusing on the improvement of security in electronic medical record systems should not only involve current but also emerging threats, adapting to technological advancements such as AI, IoT, and blockchain, which have the potential to revolutionize healthcare but also introduce new vulnerabilities.

CONCLUSION

In conclusion, the security of medical records is a complex domain shaped by technological, legal, and human factors. Enhancing their security in the face of escalating cyber threats requires a multipronged approach, incorporating cutting-edge technology, comprehensive policy frameworks, and a pervasive culture of security awareness and compliance. As healthcare continues to evolve, so too should the methodologies designed to protect the most confidential of information we possess: our health records. Achieving this will not only ensure the privacy of individuals but will also preserve the integrity of the global healthcare system at large.

REFERENCES

- Alarfaj, K. A., & Rahman, M. H. (2024). The Risk Assessment of the Security of Electronic Health Records Using Risk Matrix. *Applied Sciences, 14*(13), 5785.
- Alarfaj, K. A., & Rahman, M. H. (2024). The Risk Assessment of the Security of Electronic Health Records Using Risk Matrix. *Applied Sciences, 14*(13), 5785.
- Chen, H., Dai, W. Kim. M., & Song, Y. (2019, November). Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 395-412).
- Finlayson, S. G., Bowers, J. D. Ito. J., Zittrain, J. L., Beam, A. L., & Kohane, I. S. (2019). Adversarial attacks on medical machine learning. *Science, 363*(6433), 1287-1289.
- Greenfield, D., Pawsey, M., & Braithwaite, J. (2011). What motivates professionals to engage in the accreditation of healthcare organizations?. *International Journal for Quality in Health Care*, *23*(1), 8-14.
- Hakimi, M., Quchi, M. M., & Fazil, A. W. (2024). Human factors in cybersecurity: an in depth analysis of user centric studies. *Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)*, *3*(01), 20-33.
- Hall, M. A. (2009). Property, privacy, and the pursuit of interconnected electronic medical records. *Iowa L. Rev.*, *95*, 631.
- Hazra, R., Chatterjee, P., Singh, Y., Podder, G., & Das, T. (2024). Data Encryption and Secure Communication Protocols. In *Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning* (pp. 546-570). IGI Global.
- Jawad, L. A. (2024). "Security and Privacy in Digital Healthcare Systems: Challenges and Mitigation Strategies." *Abhigyan*, *42*(1), 23-31.
- Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egypt. Inform. J. 22*, 177–183.
- Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. *Applied sciences*, *9*(9), 1736.
- Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of medical systems*, *41*, 1-9.
- Mackey, T. K., Kuo, T. T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., ... & Palombini, M. (2019). 'Fit-for-purpose?'–challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC medicine*, *17*, 1-17.
- Mackey, T. K., Kuo, T. T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., ... & Palombini, M. (2019). 'Fit-for-purpose?'–challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC medicine*, *17*, 1-17.
- Sabry, S. S., Kaittan, N. M., & Majeed, I. (2019). The road to the blockchain technology: Concept and types. *Periodicals of Engineering and Natural Sciences (PEN)*, *7*(4), 1821-1832.
- Shaygan, A., & Daim, T. (2023). Technology management maturity assessment model in healthcare research centers. *Technovation*, *120*, 102444.
- Shaygan, A., Daim, T., (2021). Technology management maturity assessment model in healthcare research centers. *Technovation*, 102444. https://doi.org/10.1016/j.
- Tertulino, R., Antunes, N., & Morais, H. (2023). Privacy in electronic health records: A systematic mapping study. *J. Public Health*, *32*, 435–454.
- Wijayanti, D. (2024). Uncovering Security Vulnerabilities in Electronic Medical Record Systems: A Comprehensive Review of Threats and Recommendations for Enhancement. *JITEKI, 10*(1), 73-98.
- Wijayanti, D., Ujianto, E. I. H., & Rianto, R. (2024). Uncovering Security Vulnerabilities in Electronic Medical Record Systems: A Comprehensive Review of Threats and Recommendations for Enhancement. *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI)*, *10*(1), 73-98.
- Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices: *Evidence and Research*, 305-316.