JOURNAL OF HEALTHCARE SCIENCES
Volume 5 Issue 1 2025, Article ID: JOHS2025001023
http://dx.doi.org/10.52533/JOHS.2025.50106
e-ISSN: 1658-8967

Review

Privacy and Confidentiality in Healthcare: Best Practices for Protecting Patient Information

Huda Abdulqader Turkstani[1*], Fatimah Nasser Almutawah[2], Nawaf Abdulmohsen AlZamel[3], Muath Zaid Alshammari[4], Abrar Abdulrahman Alhamadi[5], Majed Talal Algharbi[6], Amer Meshari Alsuayri[7], Mohammed Badie Gong[8], Jawaher Saeed Alqahtani[9], Amani Faisal Alnemer[10], Nuha Hussein Aljuwayed[11]

[1] *Pediatric Emergency Department, East Jeddah Hospital, Jeddah, Saudi Arabia*
[2] *Emergency Department, King Fahad Hospital, Al Ahsa, Saudi Arabia*
[3] *Physical Medicine and Rehabilitation Department, Prince Sultan Military Medical City, Riyadh, Saudi Arabia*
[4] *College of Medicine, University of Hail, Hail, Saudi Arabia*
[5] *Dental Department, Alwaha Healthcare Center – Ministry of Health, Jeddah, Saudi Arabia*
[6] *Internal Medicine Department, Rabigh General Hospital, Rabigh, Saudi Arabia*
[7] *College of Medicine, University of Bisha, Bisha, Saudi Arabia*
[8] *ICU, Rabigh General Hospital, Rabigh, Saudi Arabia*
[9] *Dental Department, Pearl Clinic, Riyadh, Saudi Arabia*
[10] *College of Medicine, Alexandria University, Alexandria, Egypt*
[11] *College of Dentistry, Riyadh Elm University, Riyadh, Saudi Arabia*

Correspondence should be addressed to **Huda Abdulqader Turkstani**, Pediatric Emergency Department, East Jeddah Hospital, Jeddah, Saudi Arabia. Email: Hudaturkstani@gmail.com

Received: 14 January 2025, Revised: 19 January 2025, Accepted: 20 January 2025, Published: 22 January 2025.

Abstract

This detailed analysis explores the world of privacy and confidentiality in the healthcare industry, specifically focusing on the area of clinical management. Healthcare professionals, as guardians of patient data, must navigate the changing technology and healthcare landscape. This analysis reveals the strategies that help strike a balance in this sensitive area. A central point of the conversation emphasizes the significance of access controls through role-based access systems. These measures do not limit data access to authorized individuals. Also, adhere to the principle of least privilege by ensuring that people only view information relevant to their specific roles. Additionally, incorporating encryption technologies is crucial for protecting data during transmission and storage. Encryption provides a layer of security that prevents access and enhances overall system security in clinical management. In summary, this review outlines the strategies for safeguarding patient information security in today's evolving healthcare environment. Continuous adaptation and enhancement are not just. It is essential as the healthcare industry navigates the challenges presented by technological advancements. Healthcare providers must stay dedicated to putting patients and ensuring data security. It's crucial for them to carefully manage the line between embracing technology and protecting patient privacy.

Keyword: *Access controls, Artificial Intelligence, Clinical management, Encryption technologies, Patient Privacy*

Introduction

Ensuring privacy and confidentiality in the healthcare industry is crucial, requiring attention to safeguard data. The adoption of health records (EHRs) has significantly changed how healthcare is managed, improving access and efficiency in delivering services (1, 2). However, this digital shift also brings security challenges regarding protecting patient information (3). In research, there is an emphasis on implementing security protocols such as encryption and authentication to uphold the privacy and reliability of Electronic Health Records (EHRs). Additionally, the regulatory framework concerning data security is crucial. The regulations set by HIPAA in the United States are aimed at safeguarding data to ensure privacy and security. Research emphasizes that healthcare professionals must have an understanding of these guidelines to ensure compliance and protect data effectively (4). Organizational rules in healthcare facilities play a role in fostering a culture that values privacy and confidentiality. Training sessions and regular checks have proven to be methods for promoting a culture of privacy awareness among healthcare personnel (5, 6). By implementing these strategies, organizations aim to cultivate a sense of accountability for data across all levels, ultimately ensuring confidentiality is maintained. With the advancement of technology, innovative solutions such as blockchain, new opportunities for enhancing the security of healthcare information (7). The decentralized and tamper-proof characteristics of blockchain offer a remedy for protecting data from unauthorized access and tampering. Research indicates that exploring and integrating these emerging technologies can significantly strengthen the security of healthcare information environments. The growing interconnectedness of healthcare systems raises concerns about interoperability and its implications for patient data privacy. While seamless data exchange is crucial for healthcare delivery, ensuring confidentiality in this interconnected landscape poses challenges (8). Suggestions to tackle interoperability issues focus on standardizing data formats and protocols. Collaborative efforts at international levels are seen as vital in establishing interoperability standards that prioritize privacy (9). Despite advancements in solutions and legal frameworks, human elements continue to pose an obstacle in safeguarding patient information (10). Employee carelessness, deliberate violations, and inadequate training all play a role in creating weaknesses in the healthcare information system (11). That's why it's essential to prioritize education and training initiatives for healthcare staff. The use of Artificial Intelligence (AI) in the healthcare sector adds complexity to privacy concerns. While AI offers the potential for transforming diagnoses and treatments, it requires access to patient data (12). Balancing the advantages of AI with protecting patient privacy involves consideration and ethical guidelines. Research indicates that establishing rules for using AI in healthcare is crucial for maintaining the delicate equilibrium between technological progress and safeguarding patient information (13, 14). Overall, safeguarding data in healthcare necessitates an approach that considers technological advancements, legal frameworks, and organizational strategies. Existing literature highlights the importance of implementing security measures, complying with regulations, and fostering a culture of privacy awareness within healthcare institutions. Moreover, exploring technologies ensuring compatibility between systems and addressing factors are key components of a holistic strategy to protect patient confidentiality in the ever-evolving healthcare landscape. With advancements in healthcare, it is essential to adapt and strengthen data protection measures to uphold confidentiality and privacy effectively. This review aims to provide an overview of privacy and confidentiality in healthcare for best practices to protect patient information.

Method

Best practices for maintaining privacy and confidentiality in healthcare, particularly regarding patient information protection, were investigated. English articles from PubMed and Scopus since 2008 were reviewed, along with references cited within, to ensure inclusivity. Keywords including privacy, confidentiality, healthcare, patient

http://dx.doi.org/10.52533/JOHS.2025.50106

information, data security, and ethical considerations directed the search process.

Discussion

When it comes to discussing privacy and confidentiality in healthcare management, there are aspects that stand out as crucial elements of a successful approach. Role-based access controls are key in ensuring that authorized personnel can access data. Using encryption technologies is vital for safeguarding information when it is being transmitted or stored. Conducting audits and monitoring helps to enhance security measures, enabling healthcare organizations to quickly identify and address potential breaches. Additionally, dealing with insider threats through training programs promotes a culture of awareness and accountability among the clinical management team (15). The incorporation of Artificial Intelligence (AI), in healthcare management brings forth aspects to consider regarding privacy. To ensure that AI tools patient confidentiality it is crucial to establish guidelines and protocols. Modern healthcare systems rely on interoperability, which necessitates protocols and secure data exchange methods for seamless information sharing while protecting privacy. Furthermore, the use of telehealth and remote patient monitoring calls for communication channels and encryption to safeguard data during virtual consultations. The intricate nature of these approaches highlights the challenges in managing privacy within environments. Striking a balance between accessibility and security is essential, with technological advancements and evolving healthcare practices that demand continuous adaptation and enhancement.

Manifestation

In the evolving realm of healthcare, where advancements in technology and the sharing of health records (EHRs) are common, safeguarding the privacy and confidentiality of patient data is crucial (16). Despite regulations and established protocols breaches in privacy still occur, presenting legal and clinical dilemmas. The loss of trust between patients and healthcare providers is an outcome of breaches in data privacy (17, 18). Patients share health details with professionals, often revealing information they wouldn't disclose to anyone else. When this trust is compromised due to privacy breaches, patients may hesitate to share information, resulting in medical histories that could impact the quality of care they receive. Moreover, breaches in patient data privacy can have repercussions. Picture a scenario where a patient's confidential health information, like a health diagnosis or history of substance abuse, is disclosed without consent. This breach can evoke feelings of shame, embarrassment, and stigma, worsening the patient's health condition and deterring them from seeking treatment. From a standpoint, violations of data privacy can also cause tangible harm. Unauthorized entry into a patient's files could lead to identity theft or medical fraud. This involves making claims with the patient's details resulting in harm and possible health issues. Furthermore, when sensitive health details are shared with employers, insurers, or other parties without consent, individuals may encounter discrimination, job rejections, or insurance coverage denials based on their health condition. Apart from the impact on individuals, violations of confidentiality can also disrupt healthcare services and jeopardize patient well-being. For instance, consider a situation where a healthcare provider mistakenly accesses the records of the patient due to a system glitch or lack of proper security measures. Such errors could lead to misdiagnoses, medication mistakes, or inappropriate treatments that endanger patients' health and safety. Additionally, breaches in confidentiality can strain relationships among healthcare teams. Undermine collaborative care initiatives. Discovering privacy breaches within their institutions can erode trust among colleagues. Foster an atmosphere of suspicion and secrecy (17). This breakdown in teamwork and communication can hinder care coordination efforts, resulting in treatment approaches that may not be optimal for patients. From a perspective, violations of privacy could expose healthcare organizations to substantial financial risks and harm their reputation significantly. Regulatory bodies, such as HIPAA, impose penalties on healthcare providers and

http://dx.doi.org/10.52533/JOHS.2025.50106

institutions that violate patient privacy by not adhering to the rules. Additionally, the adverse publicity resulting from privacy violations can damage the reputation of healthcare facilities, eroding trust and potentially triggering action from those impacted. Privacy breaches in information not only violate regulations but also bring about various clinical issues. They can lead to a loss of trust and distress, jeopardize safety, and make healthcare organizations vulnerable to legal consequences. These challenges highlight the need for privacy protections and confidentiality measures in healthcare. By enforcing security protocols promoting a culture of privacy consciousness and instilling values in healthcare practitioners, we can work towards maintaining the core values of patient privacy and confidentiality in today's healthcare environment.

Management

The importance of privacy and confidentiality in healthcare in management cannot be overstated. It is essential to handle information by following protocols that protect privacy, maintain confidentiality and build trust with patients in the healthcare sector. In the field of healthcare, managing care in an environment is crucial. Safeguarding confidentiality and data privacy is vital to uphold standards and provide high quality care (19). A key aspect of management revolves around handling Electronic Health Records (EHRs) securely as they contain patient details. While EHRs facilitate patient care, striking a balance between accessibility and security is essential. Implementing access controls is a practice in clinical management. By granting role specific access to information only authorized personnel can retrieve sensitive data. Role based access control (RBAC) systems empower healthcare institutions to define roles within their management system. Allocate access rights accordingly. This not only safeguards privacy but also adheres to the principle of least privilege ensuring that individuals can only access information pertinent to their roles. Additionally utilizing encryption technologies in management helps protect the transmission and storage of data. Encrypting data both, at rest and during transmission adds a layer of security making it difficult for parties to access or intercept sensitive information. By integrating encryption into healthcare management systems, organizations improve the security of information reducing the chances of data breaches. Regular checks and monitoring play a role in clinical management when it comes to maintaining privacy and confidentiality (20, 21). Reviewing access logs and system activities periodically helps detect any occurrences or unauthorized attempts to access information. These audits are measures aimed at identifying and addressing security breaches promptly. By staying alert through surveillance healthcare institutions can safeguard data confidentiality and demonstrate a strong commitment to sound clinical management practices. Dealing with insider threats, which involve breaches originating from within the organization, is also crucial in management. Employees who have access to records can pose risks due to negligence or malicious intent. Addressing this risk involves implementing training programs and promoting a culture of awareness among healthcare staff members. Educating employees on the importance of privacy and the repercussion of access is essential for instilling a sense of accountability within the clinical management team. The incorporation of Artificial Intelligence (AI) into management systems presents opportunities well as challenges regarding privacy and confidentiality. AI tools, such as analytics, for patient outcomes rely heavily on datasets. Balancing the advantages of AI with the need to safeguard privacy requires deliberation (22). Clinical management strategies must integrate standards and frameworks governing the use of AI in a manner that upholds principles of confidentiality. We need to set up guidelines to make sure that AI programs respect privacy standards. Clinical management faces challenges, in ensuring privacy due to the growing interconnectedness of healthcare systems. The seamless exchange of data is crucial for delivering care, but it also brings up concerns about data sharing and confidentiality. To address these issues clinical management strategies must include protocols and secure data exchange methods to safeguard information during interoperable

http://dx.doi.org/10.52533/JOHS.2025.50106

processes. The integration of telehealth and remote patient monitoring adds another layer of complexity to maintaining privacy in settings. While these technologies enhance healthcare accessibility, they also raise questions about the security of transmitted data. Clinical management approaches for telehealth should prioritize communication channels encrypted data transmission and authentication measures to uphold confidentiality during virtual consultations. So, the effective clinical management of privacy and confidentiality in healthcare requires a multifaceted approach. Establishing robust access controls, implementing encryption technologies, conducting regular audits, addressing insider threats through training programs, and navigating the challenges presented by AI, interoperability, and telehealth are integral components of a comprehensive strategy. Clinical management plays a pivotal role in ensuring that patient information remains secure and confidential, ultimately contributing to the trust patients place in the healthcare system. As technology continues to advance, clinical management practices must evolve to address emerging challenges and uphold the ethical standards of patient care.

Conclusion

In conclusion, maintaining trust and ethical standards in healthcare heavily relies on managing privacy and confidentiality. A comprehensive approach includes implementing access controls, encryption technologies, regular audits, and training programs. With the rise of AI in healthcare, ethical guidelines are crucial to oversee its integration into practices. The challenges of interoperability and the growing use of telehealth highlight the need to balance data protection with accessibility. Looking ahead, healthcare institutions must stay proactive by improving their clinical management strategies to tackle obstacles. Safeguarding patient information demands collaboration among healthcare professionals, tech specialists, and policymakers. By emphasizing privacy and confidentiality in management, the healthcare industry can navigate the complexities of the era while honoring patient-centered care principles.

Disclosure

Conflict of interest

There is no conflict of interest.

Funding

No funding.

Ethical consideration

Non applicable.

Data availability

Data that support the findings of this study are embedded within the manuscript.

Author contribution

All authors contributed to conceptualizing, data drafting, collection and final writing of the manuscript.

References

1. Zarour M, Alenezi M, Ansari MTJ, Pandey AK, Ahmad M, Agrawal A, et al. Ensuring data integrity of healthcare information in the era of digital health. Healthc Technol Lett. 2021;8(3):66-77.

2. Gariépy-Saper K, Decarie N. Privacy of electronic health records: a review of the literature. J Can Health Libr Assoc. 2021;42(1):74-84.

3. Filkins BL, Kim JY, Roberts B, Armstrong W, Miller MA, Hultner ML, et al. Privacy and security in the era of digital health: what should translational researchers know and do about it? Am J Transl Res. 2016;8(3):1560-80.

4. McGraw D, Mandl KD. Privacy protections to encourage use of health-relevant digital data in a learning health system. NPJ Digit Med. 2021;4(1):2.

5. Ozdinc A, Aydin Z, Calim M, Ozkan AS, Bakir H, Akbas S. Privacy awareness among healthcare professionals in intensive care unit: A multicenter, cross-sectional study. Medicine (Baltimore). 2023;102(6):e32930.

6. Argyridou E, Nifakos S, Laoudias C, Panda S, Panaousis E, Chandramouli K, et al. Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations:

http://dx.doi.org/10.52533/JOHS.2025.50106

Concept Study. J Med Internet Res. 2023;25:e41294.

7. Ali A, Ali H, Saeed A, Ahmed Khan A, Tin TT, Assam M, et al. Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning. Sensors (Basel). 2023;23(18).

8. Esmaeilzadeh P. Evolution of Health Information Sharing Between Health Care Organizations: Potential of Nonfungible Tokens. Interact J Med Res. 2023;12:e42685.

9. Szarfman A, Levine JG, Tonning JM, Weichold F, Bloom JC, Soreth JM, et al. Recommendations for achieving interoperable and shareable medical data in the USA. Commun Med (Lond). 2022;2:86.

10. Dhirani LL, Mukhtiar N, Chowdhry BS, Newe T. Ethical Dilemmas and Privacy Issues in Emerging Technologies: A Review. Sensors. 2023;23(3):1151.

11. Pandit MS, Pandit S. Medical negligence: Coverage of the profession, duties, ethics, case law, and enlightened defense - A legal perspective. Indian J Urol. 2009;25(3):372-8.

12. Davenport T, Kalakota R. The potential for artificial intelligence in healthcare. Future Healthc J. 2019;6(2):94-8.

13. Jeyaraman M, Balaji S, Jeyaraman N, Yadav S. Unraveling the Ethical Enigma: Artificial Intelligence in Healthcare. Cureus. 2023;15(8):e43262.

14. Singam A. Revolutionizing Patient Care: A Comprehensive Review of Artificial Intelligence Applications in Anesthesia. Cureus. 2023;15(12):e49887.

15. Jalali MS, Kaiser JP. Cybersecurity in Hospitals: A Systematic, Organizational Perspective. J Med Internet Res. 2018;20(5):e10059.

16. Basil NN, Ambe S, Ekhator C, Fonkem E. Health Records Database and Inherent Security Concerns: A Review of the Literature. Cureus. 2022;14(10):e30168.

17. Beltran-Aroca CM, Girela-Lopez E, Collazo-Chao E, Montero-Pérez-Barquero M, Muñoz-Villanueva MC. Confidentiality breaches in clinical practice: what happens in hospitals? BMC Medical Ethics. 2016;17(1):52.

18. Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, Khan RA. Healthcare Data Breaches: Insights and Implications. Healthcare (Basel). 2020;8(2).

19. Jaime FJ, Muñoz A, Rodríguez-Gómez F, Jerez-Calero A. Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare. Sensors (Basel). 2023;23(21).

20. Mehrtak M, SeyedAlinaghi S, MohsseniPour M, Noori T, Karimi A, Shamsabadi A, et al. Security challenges and solutions using healthcare cloud computing. J Med Life. 2021;14(4):448-61.

21. Kruse CS, Smith B, Vanderlinden H, Nealand A. Security Techniques for the Electronic Health Records. J Med Syst. 2017;41(8):127.

22. Ahuja AS. The impact of artificial intelligence in medicine on the future role of the physician. PeerJ. 2019;7:e7702.

http://dx.doi.org/10.52533/JOHS.2025.50106