International Journal of Community Medicine and Public Health
Alhomidan ZS et al. Int J Community Med Public Health. 2025 Apr;12(4):1904-1910
http://www.ijcmph.com
pISSN 2394-6032 | eISSN 2394-6040

DOI: https://dx.doi.org/10.18203/2394-6040.ijcmph20250945

Review Article

Confidentiality in the era of electronic health records: ethical challenges and solutions

Ziad Saleh Alhomidan[1]*, Nasser Mathyab Albaqami[2], Abdulrahman Abdulkhaliq Alshehri[3], Abdullah Abdulaziz Aldubaib[4], Abdulaziz Bandar Alsuwailem[5], Khalid Faisal Al Ghadam[6]

[1]Department of Medical Administration, Ministry of Defence, Riyadh, Saudi Arabia
[2]Department of Pediatrics, Ministry of Defence, Riyadh, Saudi Arabia
[3]Department General Medicine, Ministry of Defence, Riyadh, Saudi Arabia
[4]Department of Family Medicine, King Abdulaziz Medical City, Riyadh, Saudi Arabia
[5]Department of Emergency Medicine, Ministry of Defence, Riyadh, Saudi Arabia
[6]Department of Neonatal Intensive Care Unit, Armed forces Hospital Southern Region, Khamis Mushayt, Saudi Arabia

Received: 11 March 2025
Revised: 24 March 2025
Accepted: 26 March 2025

***Correspondence:**
Dr. Ziad Saleh Alhomidan,
E-mail: Homidanz@gmail.com

ABSTRACT

The incorporation of electronic health records (EHRs) into healthcare systems has greatly enhanced medical data management efficiency and patient care. Concerning patient confidentiality, this digital transformation also raises ethical and security issues. Sensitive health information protection is a concern due to unauthorized access, cyber threats, and legal complications. Ethical principles of patient autonomy and informed consent are usually breached when patients lack control over their use of data, especially for secondary uses such as research and commercial exploitation. For enhancing security and confidentiality of EHRs, several technology alternatives have been suggested. Self-sovereign identity systems and patient-controlled data-sharing models are also being explored to enable more transparency and empower patients with greater control over their health records. Ethical dilemmas surrounding EHR confidentiality are examined in this literature review, which also looks at privacy risks, legal frameworks, and technological solutions. This review will also delve into the possibility of blockchain, artificial intelligence (AI)-powered cybersecurity, role-based access control, and encryption as viable measures for maintaining the confidentiality of EHR. By incorporating the latest research, this review aims to provide healthcare providers, policymakers, and researchers with information on how digital health privacy and security practices evolve.

Keywords: Electronic health records, Confidentiality, Encryption, Artificial intelligence, Data security

INTRODUCTION

Patient information is now stored, accessed and shared in a completely different way due to the healthcare system's quick digitization. With digital platforms that provide efficiency, accessibility and improved care coordination, EHRs or EHRs have supplanted traditional paper records as the industry standard for medical documentation. With EHRs becoming the norm for storing and sharing medical data, the development of healthcare technology has completely changed the way patient data is managed.[1] In contrast to paper-based records, EHRs facilitate instant access to patient data, enhancing clinical judgment, provider coordination, and general practice efficiency.[2,3] Even though EHRs have many advantages, there are also

serious security and ethical issues with confidentiality and illegal data access.[4]

One of the core ethical principles in healthcare is confidentiality, which guarantees that patient data is shielded from abuse and illegal access. There are now serious ethical and legal concerns regarding the protection of patient information due to the growing dependence on digital health systems, which has increased worries about illegal access, cyberthreats and misuse of private medical data EHR security lapses can result in financial fraud, identity theft, and a decline in public confidence in medical organizations.[5,6] Furthermore, who has access to patient records and how information is used for secondary purposes like research or insurance evaluations raises ethical questions.[7] Patients can trust healthcare providers to protect their personal health information because confidentiality is a fundamental principle of medical ethics. The health insurance portability and accountability act (HIPAA) in the United States and the general data protection regulation (GDPR) in Europe are two examples of the laws and regulations that governments and regulatory agencies have put in place to protect the confidentiality of EHRs.[8-10] Patient confidentiality violations are still common in healthcare settings, where hacking incidents, insider threats and systemic vulnerabilities are all contributing factors to the rise in data breaches. It is still difficult to ensure compliance despite these legal frameworks, particularly given the growing sophistication of cyberthreats. Furthermore, new risks and opportunities arise as blockchain, cloud computing, and AI continue to influence digital healthcare.[10] The possibility of illegal access is one of the main ethical issues with EHRs. Different administrative and medical personnel frequently have different levels of access to patient data, which could pose privacy risks if access controls are not appropriately implemented. Healthcare organizations face an ethical conundrum when attempting to strike a balance between the necessity of sharing information and maintaining patient privacy. The rise of cloud-based storage options, AI and big data analytics has also raised fresh questions about data ownership and the secondary use of patient data.[11] Although large datasets are necessary for AI-driven predictive analytics and research projects to enhance clinical and public health outcomes, the opaqueness of data usage raises concerns regarding patient autonomy, informed consent and ethical governance.[12]

Examining security risks, evaluating legal and policy frameworks that control patient data protection and analyzing the ethical issues surrounding EHR confidentiality are the objectives of this literature review.

It will also showcase new developments in technology and risk-reduction best practices such as blockchain encryption, AI-powered cybersecurity and improved access control systems. By combining the most recent findings, this review will shed light on how the ethics of digital health are developing and offer ways to protect patient privacy in the age of the electronic medical records.

LITERATURE SEARCH

The Cochrane Library, PubMed, ProQuest, and Google Scholar, and other databases were used to perform a thorough literature search. To ensure the inclusion of the most recent and pertinent studies, the search was restricted to peer-reviewed publications released between 2015 and 2024. The following medical subject headings (MeSH) were used: “electronic health records”, “confidentiality in healthcare”, “data security”, “EHRs Privacy”, “ethics in digital health”, “cybersecurity in healthcare” and “HIPAA and GDPR compliance”. Clinical studies, systematic reviews, policy analyses and ethical discussions addressing confidentiality issues in EHRs were among the inclusion criteria. Studies that only looked at non-healthcare settings or paper-based records were not included. Furthermore, references from important articles were manually vetted to guarantee thorough discussion of the subject.

DISCUSSION

Ethical challenges in EHR confidentiality

Unauthorized access and insider threats

Unauthorized access remains one of the primary threats to EHR confidentiality.[13] Unlike paper records, which require physical access, EHR systems are accessible remotely, increasing the risk of exposure to unauthorized individuals.[14,15] Insider threats, where employees misuse their access privileges, are particularly concerning.[16] Studies indicate that internal data breaches often exceed external cyberattacks in frequency, with employees accessing patient records for personal curiosity, financial gain, or even identity theft.[17,18] Additionally, healthcare institutions face challenges in ensuring compliance with access control policies. Many hospitals implement monitoring tools to track user access, but these measures often lack real-time threat detection capabilities. AI-powered monitoring systems are emerging as a solution, identifying unusual behavior patterns and preventing insider threats before they occur.[19,20]

Cybersecurity threats and data breaches

The increasing digitization of healthcare records has led to a surge in cyberattacks targeting EHR systems.[21-23] Cybercriminals exploit vulnerabilities through ransomware, phishing schemes, and malware, often disrupting hospital operations and compromising patient data.[24] Healthcare data is particularly attractive to attackers due to its high value on the black market, where stolen medical records can be used for identity fraud and insurance scams.[25] One emerging concern is the rise of

deepfake phishing attacks, where cybercriminals use AI-generated voices and emails that mimic hospital executives to trick employees into providing login credentials.[26] To combat these threats, institutions are investing in advanced security measures such as biometric authentication, zero-trust security frameworks, and AI-driven anomaly detection that monitors for unauthorized access attempts in real-time.[27]

Legal and regulatory challenges

Regulatory frameworks such as HIPAA in the U.S. and GDPR in Europe impose strict guidelines on healthcare data protection, but compliance remains an ongoing challenge.[28] Many healthcare providers struggle to align with these regulations due to evolving cybersecurity threats and resource constraints.[29,30] In developing countries, limited digital infrastructure further complicates adherence to international privacy laws, leaving patient data at higher risk of exploitation. Another major challenge is the cross-border exchange of medical records, especially for patients receiving care in multiple countries.[31] Conflicting privacy laws create legal uncertainty, making it difficult for healthcare organizations to share patient data securely.[32] Future policy efforts should focus on creating standardized international regulations that promote both security and accessibility in healthcare data management.

Informed consent and secondary data use

EHRs allow seamless data sharing among healthcare providers, insurers, and researchers, but concerns remain about the extent to which patient data is used for secondary purposes.[33,34] Many patients are unaware that their medical records are often shared with third parties for research, clinical trials, and pharmaceutical development without explicit consent. This raises ethical concerns about patient autonomy and data ownership. Emerging solutions include patient-controlled data-sharing platforms that allow individuals to grant or restrict access to their records based on specific purposes.[35,36] Additionally, blockchain-based consent management systems are being explored to enhance transparency and allow patients to track how their health data is used over time.[37,38]

Strategies to maintain EHR privacy

Data storage that is secure and encrypted

One of the best ways to protect patient information from unwanted access is through encryption.[39] End-to-end encryption ensures that Sensitive health information is protected even if it is intercepted during transmission.[40] Future-proofing EHR security against possible quantum computing threats is being investigated through developments in quantum-resistant encryption algorithms. For the protection of EHR data, decentralized storage options like blockchain are also becoming more popular.[41] Tamper-proof records are made possible by blockchain technology, which makes it impossible for unauthorized changes to take place undetected. Healthcare organizations are starting to use hybrid cloud-blockchain models to combine the security advantages of decentralized data management with the scalability of cloud computing.[42]

RBAC stands for role-based access control

RBAC, which restricts user permissions according to their job role, is still a crucial tactic for stopping illegal data access.[43,44] Nonetheless, there are still issues with making sure that access privileges are updated frequently when employee roles shift. Data breaches are more likely to occur in hospitals that neglect to remove access for former workers or modify permissions for role changes. AI-driven identity and access management (IAM) systems are being used to automate real-time user permission updates to address this.[45] By identifying and flagging irregularities in workflow patterns, these systems make sure that workers only have access to the information required for their jobs.[46]

Biometric security and multi-factor authentication

Multi-factor authentication (MFA) provides an essential security layer by requiring several verification steps before allowing access to EHR systems.[47] Newer techniques incorporate biometric verification such as retinal scans and heartbeat authentication, while more conventional MFA techniques rely on SMS or email authentication.[48] But there are still implementation issues, especially with user compliance. In emergencies, extra authentication steps can be difficult for certain medical professionals. Hospitals are investigating adaptive MFA which modifies authentication requirements according to risk levels as a way to strike a balance between security and efficiency. For instance, regular logins from reliable sources might only need one verification step but attempts at high-risk access might necessitate extra security.

Privacy controls centered on the patient

Trust in EHR systems is increased when patients are given the ability to manage their health data. Individuals can now choose which healthcare organizations or providers have access to their records, through the granular privacy settings available on many contemporary patient portals.[49,50] According to research, patient-centered privacy controls increase transparency, autonomy, and trust, which increases people's propensity to use digital health platforms. HR systems frequently have patient portals that give users real-time access to their test results, treatment plans and medical history. To increase transparency, some systems also allow Patients to change permissions, choose who can access their

records, and get real-time notifications when healthcare providers access their data through these portals, which provide different levels of control. EHR systems frequently offer few options for controlling or limiting access to specific data, even though many of them let patients view their records. In certain situations, patients might not have complete control over how their data is shared with researchers, insurance companies, or other third parties or the ability to amend or remove it. Due to this lack of control, there are now worries about illegal access to healthcare organizations making money off of patient data, and the moral ramifications of using patient data for unrelated purposes. To provide patients with full control over their medical data, self-sovereign identity (SSI) frameworks are being investigated.[51] SSI enables people to keep and control their medical records on their own devices, allowing access only when required.[52] In digital healthcare, patient confidentiality may be redefined by this decentralized strategy.

Frequent training on compliance and security audits

To find weaknesses in EHR systems, regular security audits are essential. By carrying out penetration testing in which ethical hackers try to get past security measures, healthcare organizations can improve their cybersecurity protocols.[53] Studies show that human error, such as using weak passwords, sharing login information, and being vulnerable to phishing attacks, is responsible for a sizable percentage of security incidents. Cybersecurity training programs have been widely implemented in healthcare organizations to counter this, teaching healthcare workers how to protect patient data, spot phishing attempts, and comply with regulations. Organizations with regular cybersecurity training have been found to have fewer breaches and faster incident response times than those with little training. Additionally, real-time monitoring systems that notify security teams of unwanted access attempts are now being implemented in hospitals. Healthcare organizations can greatly strengthen their defense against insider threats and external cyberattacks by combining advanced security with continuous staff training. AI driven solutions are also being introduced to identify suspicious login behaviors such as access from multiple locations or excessive data retrieval attempts.

Emerging trends and future directions

New methods for improving EHR confidentiality are appearing as technology develops further.[54] Blockchain generation has acquired large interest primarily based on its tamper-proof and decentralized nature, which allows continuous retention of records, more advantageous information integrity, and better transparency in patient health records.[55] Through the elimination of a single factor of failure, blockchain is capable of saving from unauthorized access and information breaches and ensure that personal information is secure but reachable in an easy and verifiable way. In addition, predictive analytics and AI are also at the center of proactive cybersecurity. AI fashions can detect capacity safety dangers in real-time by way of means of monitoring anomalous access patterns, detecting vulnerabilities, and blocking unauthorized access earlier than any breaches occur. Machine learning of algorithms may be carried out to automate monitoring of EHR access logs, flagging any suspicious activity that might suggest a breach. Another critical fashion is the harmonization of worldwide privacy policies and legal guidelines to facilitate secure worldwide information exchange at the same time as keeping sturdy confidentiality safety measures.[56] With the worldwide transport of healthcare turning into more and more interdependent, improvement of interoperable information safety schemes (inclusive of more potent GDPR compliance, HIPAA compliance, and WHO virtual fitness standards) is critical to facilitate more cross-border sharing of healthcare information without infringing on the confidentiality of patients.[57] Besides, rising encryption strategies inclusive of homomorphic encryption and quantum cryptography provide new approaches of defensive EHR information [58]. Homomorphic encryption allows steady processing of information without decryption, lowering the hazard of publicity during information transmission. Meanwhile, quantum-resistant encryption is being studied as a future-proofing approach to fight continuously evolving cyber threats.

CONCLUSION

The ethical issues raised by EHR confidentiality necessitate a multifaceted strategy that strikes a balance between privacy protection and data accessibility. Issues with cyber threats, unauthorized access, and regulatory compliance emphasize the necessity of strong security frameworks. Multi-factor authentication, encryption, role-based access control, and patient-centered privacy measures are all workable ways to protect patient data. Retaining patient confidentiality and professional integrity in digital healthcare requires addressing these ethical issues. Future studies should concentrate on enhancing patient participation in data privacy decisions, integrating AI-driven security systems, and improving regulatory policies. Healthcare organizations can prioritize confidentiality and ethical responsibility while navigating the rapidly changing landscape of HERs by taking proactive steps.

Funding: No funding sources
Conflict of interest: None declared
Ethical approval: Not required

REFERENCES

1. Stoumpos AI, Kitsios F, Talias MA. Digital transformation in healthcare: technology acceptance and its applications. Int J Environmen Res Publ Heal. 2023;20(4):3407.

2. Li E, Clarke J, Ashrafian H, Darzi A, Neves AL. The impact of electronic health record interoperability on safety and quality of care in high-income countries: systematic review. J Med Internet Res. 2022;24(9):e38144.
3. Al-Shammari MA, Jaafar JS, Elfeshawy R. The role of electronic health records in improving pediatric nursing care: a systematic review. Egypt Pediatr Asso Gazette. 2024;72(1):77.
4. Javaid M, Haleem A, Singh RP. Health informatics to enhance the healthcare industry's culture: An extensive analysis of its features, contributions, applications and limitations. Inform Health. 2024;1(2):123-48.
5. Osawaru G. Electronic Health Record Data Breaches in US Healthcare Industry: A Quantitative Study Using the Protection Motivation Theory (PMT) to Mitigate Data Breaches, University of the Cumberlands. 2024.
6. Mancho AT. A case study on data insecurity in automated medical record security lapses. Northcentral University; 2015.
7. Snellings E. Cyber Threats on the Electronic Healthcare Record System, Utica College. 2020.
8. Stadler A. The Health Insurance Portability and Accountability Act and its Impact on Privacy and Confidentiality in Healthcare. 2021.
9. Marovic B, Curcin V. Impact of the European general data protection regulation (GDPR) on health data management in a European Union candidate country: a case study of Serbia. JMIR Med Informat. 2020;8(4):e14604.
10. Yuan B, Li J. The policy effect of the General Data Protection Regulation (GDPR) on the digital public health sector in the European Union: an empirical investigation. Int J Environ Res Publ Heal. 2019;16(6):1070.
11. Khan ZF, Alotaibi SR. Applications of artificial intelligence and big data analytics in m-health: A healthcare system perspective. J Healthcare Enginring. 2020;2020(1):8894694.
12. Mondal H, Mondal S. Ethical and social issues related to AI in healthcare. Methods Microbiol. 2024;55:247-81.
13. Banerjee S, Barik S, Das D, Ghosh U. EHR security and privacy aspects: A systematic review. IFIP International Internet of Things Conference. 2023.
14. Alarfaj KA, Rahman MH. The Risk Assessment of the Security of Electronic Health Records Using Risk Matrix. Applied Sci. 2024;14(13):5785.
15. Sharma P, Bir J, Prakash S. Navigating Privacy and Security Challenges in Electronic Medical Record (EMR) Systems: Strategies for Safeguarding Patient Data in Developing Countries-A Case Study of the Pacific. Paper presented at: International Conference on Medical Imaging and Computer-Aided Diagnosis. 2023.
16. Brown LT. Human factors and the insider threat to electronic health records: A case study, Northcentral University. 2018.
17. Burks A. Strategies Used in Healthcare Organizations to Protect Information Against Security Breaches: A Case Study, University of Phoenix. 2024.
18. Seh AH, Zarour M, Alenezi M, Amal KS, Alka A, Rajeev K, et al. Healthcare data breaches: insights and implications. Healthcare. 2020;8(2):133.
19. Alshamrani M. IoT and artificial intelligence implementations for remote healthcare monitoring systems: A survey. J King Saud University Computer Information Sci. 2022;34(8):4687-701.
20. Paraschiv E-A, Cîrnu CE, Vevera AV. Integrating Artificial Intelligence and Cybersecurity in Electronic Health Records: Addressing Challenges and Optimizing Healthcare Systems. 2024.
21. Paul M, Maglaras L, Ferrag MA, Almomani I. Digitization of healthcare sector: A study on privacy and security concerns. ICT Express. 2023;9(4):571-88.
22. Nemec Zlatolas L, Welzer T, Lhotska L. Data breaches in healthcare: security mechanisms for attack mitigation. Cluster Computing. 2024;27(7):8639-54.
23. Ala'a M, Ramayah T, Al-Sharafi MA. Exploring the impact of cybersecurity on using electronic health records and their performance among healthcare professionals: A multi-analytical SEM-ANN approach. Technol Society. 2024;77:102592.
24. Neprash HT, McGlave CC, Cross DA, Beth AV, Michael AP, Jared DH, et al. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. JAMA Health Forum. 2022;3(12):e224873.
25. Koppel R, Kuziemsky C. Healthcare data are remarkably vulnerable to hacking: connected healthcare delivery increases the risks. In: Improving Usability, Safety and Patient Outcomes with Health Information Technology. IOS Press. 2019;218-22.
26. Alugoju NR. The Dark Side Of Ai: A Growing Globalthreat In Cybersecurity. International Journal Of Engineering And Technology Research (IJETR). 2024;9(2):579-87.
27. Poongodi R, Samuel R, Rohith P, Parthasarathy S, Ramana B. Strengthening Cybersecurity in Indian Healthcare–Lessons from the Recent Ransomware Attacks on Hospitals. IJARIIT. 2024;16(6):NA.
28. Isibor E. Regulation of Healthcare Data Security: Legal Obligations in A Digital Age. Faculty Of Law In Partial Fulfilment Of The Requirement For The Award Of Bachelor Of Laws (Ll.B) Of Obafemi Awolowo University Ile-Ife, Osun State, Nigeria. 2024;1-132.
29. Alanazi AT, Alanazi A. Clinicians' perspectives on healthcare cybersecurity and cyber threats. Cureus. 2023;15(10):e47026.
30. Nifakos S, Chandramouli K, Nikolaou CK, et al. Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors. 2021;21(15):5119.
31. Marušič D, Rupel VP, Mihelj P. Cross-Border Experiences in Health IT: What Are the Requests for

the Medical Record? Opportunities and Emerging Issues. Paper presented at: New Perspectives in Medical Records: Meeting the Needs of Patients and Practitioners. 2017.
32. Nalin M, Baroni I, Faiella G, Maria R, Flavia M, Erol G, et al. The European cross-border health data exchange roadmap: Case study in the Italian setting. J Biomed Informat. 2019;94:103183.
33. De Moor G, Sundgren M, Kalra D, Andreas S, Martin D, Brecht C, et al. Using electronic health records for clinical research: the case of the EHR4CR project. J Biomed Informat. 2015;53:162-73.
34. Shah SM, Khan RA. Secondary use of electronic health record: Opportunities and challenges. IEEE. 2020;8:136947-65.
35. Cobrado UN, Sharief S, Regahal NG, Zepka E, Mamauag M, Velasco LC. Access control solutions in electronic health record systems: A systematic review. Informat Med Unlocked. 2024;101552.
36. Cascini F, Pantovic A, Al-Ajlouni YA, Puleo V, De Maio L, Ricciardi W. Health data sharing attitudes towards primary and secondary use of data: a systematic review. EClinicalMedicine. 2024;71.
37. Omar IA, Jayaraman R, Salah K, Simsekler MCE, Yaqoob I, Ellahham S. Ensuring protocol compliance and data transparency in clinical trials using Blockchain smart contracts. BMC Med Res Methodol. 2020;20:1-17.
38. Esmaeilzadeh P, Mirzaei T. The potential of blockchain technology for health information exchange: experimental study from patients' perspectives. J Med Internet Res. 2019;21(6):e14184.
39. Abhishek, Tripathy HK, Mishra S. A succinct analytical study of the usability of encryption methods in healthcare data security. In: Next generation healthcare informatics. Springer. 2022;105-20.
40. Chen F, Luo Y, Zhang J, Junru Z, Ziyang Z, Chuanxin Z,et al. An infrastructure framework for privacy protection of community medical internet of things: Transmission protection, storage protection and access control. World Wide Web. 2018;21(1):33-57.
41. Dubovitskaya A, Baig F, Xu Z, Rohit S, Pratik SZ, Arun S, et al. ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care. Journal of medical Internet research. 2020;22(8):e13598.
42. Shuaib K, Abdella J, Sallabi F, Serhani MA. Secure decentralized electronic health records sharing system based on blockchains. J King Saud University Computer Inform Sci. 2022;34(8):5045-58.
43. Hu VC, Ferraiolo D, Kuhn DR. Assessment of access control systems. Vol 76: US Department of Commerce, National Institute of Standards and Technology. 2006.
44. Samonte MJC, Dalina CQ, Pingol YEM, Yee FNME. Secure Healthcare Access: Design and Implementation of a Web Application through Role-Based Access Control in an Integrated Diagnostic Health Center. Paper presented at: 2024 14th International Conference on Software Technology and Engineering (ICSTE). 2024.
45. Hämäläinen M. Analysis of artificial intelligence in cybersecurity identity and access management: potential for disruptive innovation. Lappeenranta–Lahti University of Technology LUT Master's Programme in Software Product Management and Business, Master's thesis. 2024.
46. Fareed G, Faiza KES, Johnson E. AI-Powered IAM Solutions for Strengthening HIPAA Compliance in Cloud-Based Healthcare Systems. Int J Adv Engineering Technol Innovations. 2021;1(4):118-45.
47. Chaudhari S, Tomar S, Rawat A. Design, implementation and analysis of multi layer, Multi Factor Authentication (MFA) setup for webmail access in multi trust networks. Paper presented at: 2011 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC). 2011.
48. Carmel V, Akila D. A survey on biometric authentication systems in cloud to combat identity theft. J Crit Rev. 2020;7(03):540-7.
49. Saks MJ, Grando A, Murcko A, Millea C. Granular patient control of personal health information: federal and state law considerations. Jurimetrics. 2018;58(4):411.
50. Nowrozy R, Ahmed K, Kayes A, Wang H, McIntosh TR. Privacy preservation of electronic health records in the modern era: A systematic survey. ACM Computing Surveys. 2024;56(8):1-37.
51. Siqueira A, Da Conceição AF, Rocha V. Blockchains and self-sovereign identities applied to healthcare solutions: A systematic review. ACM Comput Surv. 2021;1(1):1-28.
52. Bai P, Kumar S, Aggarwal G, Mahmud M, Kaiwartya O, Lloret J. Self-sovereignty identity management model for smart healthcare system. Sensors. 2022;22(13):4714.
53. Ettaloui N, Arezki S, Gadi T. Blockchain-Based Electronic Health Record: Systematic Literature Review. Human Behavior Emerging Technologies. 2024;2024(1):4734288.
54. Negro-Calduch E, Azzopardi-Muscat N, Krishnamurthy RS, Novillo-Ortiz D. Technological progress in electronic health record system optimization: Systematic review of systematic literature reviews. Int J Med Informatics. 2021;152:104507.
55. Rashid MRA, Al Rafi A, Islam MA, Sharkar SU, Rafi ZH, Hasan M, et al. Enhancing land management policy in Bangladesh: A blockchain-based framework for transparent and efficient land management. Land Use Policy. 2025;150:107436.
56. Alhasan TK. Managing legal risks in health information exchanges: A comprehensive approach to privacy, consent, and liability. J Healthcare Risk Management. 2025;NA.
57. Xia L, Cao Z, Zhao Y. Paradigm Transformation of Global Health Data Regulation: Challenges in

Governance and Human Rights Protection of Cross-Border Data Flows. Risk Management Healthcare Policy. 2024;17:3291-304.
58. Sabonchi AKS. Securing Electronic Health Records with Cryptography and Lion Optimization. J Cyber Security. 2025;7(1):21-43.

Cite this article as: Alhomidan ZS, Albaqami NM, Alshehri AA, Aldubaib AA, Alsuwailem AB, Al Ghadam KF. Confidentiality in the era of electronic health records: ethical challenges and solutions. Int J Community Med Public Health 2025;12:1904-10.