RESEARCH PAPER

Advantages and Constraints of Electronic Health Records in Safeguarding Patient Data and Privacy: A Review

Mrs. Lipika Maiti[1*], Dr. Umesh Kumar Sharma[2]

[1*] Ph.D. Scholar, LN Nursing College, LNCT University, Bhopal, Madhya Pradesh, India (Corresponding Author).
Email: lipikam6@gmail.com

[2] Professor, LN Nursing College, LNCT University, Bhopal, Madhya Pradesh, India

Received: 12th Mar, 2026 | **Revised:** 24th Mar, 2026 | **Accepted:** 14th Apr, 2026 | **Available Online:** 30th Apr, 2026

ABSTRACT

Background:

The widespread adoption of electronic health records (EHRs) has improved healthcare delivery but has also raised important concerns regarding data security and patient privacy.

Objective:

To examine the advantages and limitations of EHRs in protecting patient data and to explore approaches for strengthening digital health security.

Methods:

A narrative review was conducted using PubMed/MEDLINE, Scopus, Web of Science, Embase, CINAHL, Google Scholar, ScienceDirect, IEEE Xplore, and Cochrane Library. Studies published between 2020 and 2026 were included. Data were synthesized using a thematic approach.

Results:

EHRs improve accessibility, documentation accuracy, and data management through controlled access, audit trails, encryption, and backup systems. However, challenges such as cybersecurity threats, unauthorized access, interoperability risks, technical vulnerabilities, and ethical concerns remain significant. Emerging technologies including artificial intelligence, blockchain, cloud security, biometric authentication, and zero-trust models show potential, although practical implementation remains limited.

Conclusion:

EHRs support better protection of patient data, but effective security requires integrated technical, organizational, and policy-level measures.

Keywords: Electronic Health Records, Patient Privacy, Data Security, Cybersecurity, Health Information Systems, Data Protection, Digital Health.

How to cite this article: Maiti L, Sharma UK. Advantages and Constraints of Electronic Health Records in Safeguarding Patient Data and Privacy: A Review. Int J Drug Deliv Technol. 2026;16(39s): 539-549. DOI: 10.25258/ijddt.16.39s.73

Source of support: Nil.

Conflict of interest: None

INTRODUCTION

The rapid digitization of healthcare has led to widespread adoption of electronic health records (EHRs), transforming management, storage, and exchange of patient information[1]. EHR systems enable comprehensive and longitudinal documentation of clinical data, improving accessibility, standardization, and interoperability across healthcare settings. These capabilities support enhanced clinical decision-making, continuity of care, and overall healthcare efficiency[2].

However, the increasing reliance on digital health systems has intensified concerns regarding data security and patient privacy. Healthcare data are highly sensitive and valuable, making EHR systems a frequent target for cyber threats, including data breaches, ransomware attacks, and unauthorized access[3]. In addition to external risks, internal vulnerabilities such as

human error, inadequate training, and weak access control mechanisms further compromise the confidentiality and integrity of patient information. Ensuring the protection of health data while maintaining accessibility for clinical use remains a critical challenge in modern healthcare systems[4].

The growing integration of interconnected systems, cloud-based platforms, and advanced technologies has further increased the complexity of safeguarding patient information. Variations in technological infrastructure, regulatory frameworks, and resource availability across healthcare systems contribute to differences in data protection practices[5]. Ethical considerations related to data ownership, informed consent, and secondary use of health information also play a significant role in shaping privacy and security in digital healthcare environments[6].

In this context, a comprehensive evaluation of electronic health records is essential to understand their role in safeguarding patient data and privacy. This review examines the advantages and constraints of EHR systems and explores emerging strategies to strengthen data security and confidentiality in digital healthcare systems.

BACKGROUND AND CONCEPTUAL BASIS

Evolution of Electronic Health Records

The transition from paper-based documentation to electronic health records (EHRs) represents a major shift in healthcare information management. Traditional paper records were fragmented, prone to loss, and limited in accessibility, constraining continuity of care and data sharing[7]. The evolution of computerized health systems, initially developed for administrative functions, has progressively enabled integration of clinical data into unified digital platforms. The global adoption of EHRs has accelerated through policy-driven initiatives and increasing demand for data-driven healthcare[8]. While high-income countries have achieved more advanced implementation, low- and middle-income settings continue to face challenges related to infrastructure, interoperability, and resource constraints. EHR systems now play a central role in enhancing care coordination, improving data accuracy, and supporting evidence-based clinical and public health decision-making[9].

Definition and Core Components of EHR

Electronic health records are structured digital systems that store and manage patient health information over time, enabling secure and interoperable data exchange across healthcare providers. Unlike institution-specific electronic medical records, EHRs are designed for longitudinal and cross-system integration[10]. Core components include patient demographics, clinical history, medication records, diagnostic data, and administrative information. These elements support clinical decision-making, reduce medical errors, and improve workflow efficiency. Interoperability remains a defining feature, facilitating seamless data exchange across systems, although it introduces challenges related to standardization, compatibility, and data security[11].

Concepts of Patient Data Security and Privacy

The protection of patient data within EHR systems is based on the principles of confidentiality, integrity, and availability. Confidentiality ensures restricted access to authorized users, integrity maintains data accuracy and consistency, and availability supports timely access for clinical use. While security refers to the technical and organizational measures used to protect data, privacy relates to individuals' rights over the use and sharing of their information[12]. The increasing complexity of digital health systems, including interconnected platforms and advanced technologies, has intensified concerns regarding data ownership, informed consent, and accountability. Effective EHR systems require alignment of technical safeguards with ethical and regulatory frameworks to ensure secure and responsible data management[13].

OBJECTIVE

This review aims to examine the advantages and limitations of electronic health records in protecting patient data and privacy.

MATERIAL AND METHODOLOGY

Study Design and Approach

This study was conducted as a narrative review with systematic search and selection elements to synthesize evidence on electronic health records (EHRs), patient privacy, and data security. The approach enabled integration of multidisciplinary literature while maintaining methodological transparency.

Search Strategy

A comprehensive and systematic literature search was conducted across multiple electronic databases, including PubMed/MEDLINE, Scopus, Web of Science, Embase, CINAHL, Google Scholar, Cochrane Library, IEEE Xplore, and ScienceDirect. The search covered studies published between 2010 and 2025. A combination of Boolean operators and controlled vocabulary terms was used to optimize retrieval. The

search strategy included terms such as “electronic health records” OR “EHR” AND “patient privacy” OR “data security” OR “confidentiality” AND “cybersecurity” OR “data breach” OR “health information security.”

Study Area and Scope

The review adopts a global perspective, examining electronic health record (EHR) implementation across diverse healthcare settings, including high-income and low- and middle-income countries. It focuses on technological, ethical, legal, and organizational aspects of data security, including access control, interoperability risks, and emerging digital health technologies.

Inclusion and Exclusion Criteria

Peer-reviewed original studies and review articles published between 2020 and 2026 focusing on EHR systems, patient privacy, and data security were included. Studies across multiple designs were considered. Editorials, commentaries, non-relevant studies, non-English publications, and articles without accessible full text were excluded.

Study Selection Process

Studies were selected based on relevance to EHR-related privacy and data security. Titles and abstracts were screened, followed by full-text evaluation to confirm inclusion. Duplicate records were removed, and studies containing detailed information on EHR systems and data protection were included for final synthesis.

ADVANTAGES OF EHRs IN SAFEGUARDING PATIENT DATA AND PRIVACY

- **Improved Accessibility with Controlled Authorization:** Electronic health records (EHRs) enable rapid and real-time access to patient information, significantly enhancing clinical efficiency and decision-making. Unlike paper-based systems, EHRs utilize role-based access controls, ensuring that only authorized personnel can view or modify specific data elements. This controlled accessibility minimizes unnecessary exposure of sensitive information while facilitating coordinated care across multiple healthcare providers[14].
- **Enhanced Documentation Accuracy and Legibility:** EHRs improve the quality of clinical documentation by eliminating issues related to illegible handwriting and incomplete records. Standardized templates and structured data entry ensure consistency, accuracy, and completeness of patient information. This reduces clinical errors, enhances communication among healthcare professionals, and supports safer patient care[15].
- **Audit Trails and Monitoring:** A key advantage of EHR systems is the ability to maintain detailed audit trails that record all user interactions with patient data. These logs enable tracking of who accessed, modified, or transmitted information, thereby enhancing transparency. Audit mechanisms facilitate early detection of unauthorized access and promote accountability among healthcare staff, strengthening data governance practices[16].
- **Data Backup and Disaster Recovery:** EHR systems incorporate robust data backup and disaster recovery mechanisms, significantly reducing the risk of data loss associated with physical records. Cloud-based storage and secure server backups ensure that patient information can be restored in the event of system failure, natural disasters, or accidental damage. This enhances data continuity and resilience of healthcare systems[17].
- **Encryption and Authentication Mechanisms:** Advanced security features, such as data encryption and authentication protocols, are integral to EHR systems. Encryption ensures secure transmission and storage of sensitive health information, protecting it from unauthorized interception. Authentication measures, including password protection and multi-factor authentication, further strengthen system security by verifying user identity before granting access[18].
- **Support for Regulatory Compliance:** EHRs facilitate adherence to legal and regulatory requirements related to patient data protection. They enable systematic documentation of patient consent, access logs, and data usage, which are essential for compliance with privacy regulations. Additionally, EHR systems support monitoring and auditing by regulatory bodies, ensuring accountability and standardization in data management practices[19].
- **Patient Engagement and Transparency:** EHRs promote patient-centered care by enhancing engagement and transparency through features such as patient portals. These platforms allow individuals to access their health records, review treatment plans, and monitor clinical progress. Controlled access to personal health information fosters trust, improves patient involvement in care decisions, and enhances overall satisfaction[20].
- **Reduction of Duplication and Fragmentation:** By centralizing patient information, EHRs reduce duplication of records and fragmentation of care.

Integrated systems enable seamless sharing of information among authorized providers, minimizing repeated diagnostic tests and redundant procedures. This not only improves efficiency but also enhances patient safety by ensuring continuity and consistency of care[21].

CONSTRAINTS AND CHALLENGES OF EHRS IN SAFEGUARDING PATIENT DATA AND PRIVACY

- **Cybersecurity Threats:** Despite advanced security mechanisms, EHR systems remain highly vulnerable to cyberattacks. Threats such as hacking, ransomware, phishing, and malware compromise the confidentiality and integrity of patient data. Large-scale data breaches in healthcare highlight the increasing attractiveness of health information to cybercriminals due to their high economic and identity value[22].
- **Unauthorized Access and Insider Misuse:** Internal threats represent a significant challenge to EHR security. Unauthorized access due to staff curiosity, weak password practices, and improper sharing of login credentials can lead to privacy violations. Human error, including accidental data disclosure or incorrect data handling, further exacerbate the risk of breaches within healthcare organizations[23].
- **Interoperability-Related Privacy Risks:** While interoperability enhances care coordination, it introduces additional privacy risks through data exchange across multiple systems and platforms. Integration with third-party vendors and external systems expands the attack surface, increasing the likelihood of unauthorized access or data leakage if security standards are inconsistent or poorly implemented[24].
- **Inadequate User Training:** A lack of cybersecurity awareness among healthcare professionals significantly undermines the effectiveness of EHR security systems. Inadequate training leads to improper documentation practices, poor password management, and non-adherence to privacy protocols. Human factors remain one of the weakest links in maintaining data security[25].
- **Technical Vulnerabilities:** Technical limitations such as outdated software, poorly configured systems, and weak encryption mechanisms expose EHR systems to potential exploitation. System downtime and infrastructure failures can also compromise data availability and disrupt clinical workflows, impacting both security and patient care[26].
- **Consent and Ethical Concerns:** EHR systems raise complex ethical issues related to patient autonomy and data governance. Concerns include secondary use of patient data for research or commercial purposes, inadequate informed consent processes, and ambiguity regarding ownership of health information. Balancing data accessibility for care and research with privacy protection remains a critical ethical challenge[27].

Financial and Infrastructure Constraints: The implementation and maintenance of secure EHR systems require substantial financial investment. High costs associated with infrastructure, software, and cybersecurity measures limit adoption, particularly in low- and middle-income countries. Additionally, limited technical expertise and resources hinder effective implementation and ongoing system security[28].

COMPARATIVE ANALYSIS OF PAPER RECORDS AND ELECTRONIC HEALTH RECORDS (EHRS)

A comparative evaluation of paper-based records and electronic health records (EHRs) is essential to understand their relative strengths and limitations in safeguarding patient data and privacy. While paper records offer inherent protection against cyber threats due to their physical nature, they are vulnerable to loss, damage, and unauthorized physical access. In contrast, EHRs provide advanced security features, improved accessibility, and better care coordination, but introduce risks related to cybersecurity and system vulnerabilities. The effectiveness of EHRs in protecting patient data largely depends on proper implementation, robust security measures, and governance frameworks[29].

Table 1 Comparative Analysis of Paper Records and Electronic Health Records (EHRs) in Patient Data Privacy and Security[29].

Domain	Paper Records	Electronic Health Records (EHRs)
Accessibility	Limited to physical location; time-consuming retrieval	Rapid, real-time access across multiple settings
Privacy Strengths	Restricted physical access reduces large-scale exposure	Role-based access, authentication, and encryption enhance privacy
Security Mechanisms	Physical locks and manual control	Passwords, multi-factor authentication,

		encryption, audit trails
Unauthorized Access Risk	Physical theft or unauthorized viewing	Hacking, phishing, weak passwords, insider misuse
Audit and Monitoring	No tracking of access or changes	Comprehensive audit trails and monitoring systems
Data Integrity and Accuracy	Prone to illegibility and incomplete records	Standardized, accurate, and legible documentation
Data Loss Risk	High risk due to fire, flood, or misplacement	Reduced risk due to backups and disaster recovery systems
Interoperability	Limited or absent	Seamless data exchange across systems
Cybersecurity Risks	Not vulnerable to cyberattacks	Vulnerable to cyber threats and data breaches
Operational Efficiency	Slow, duplication of records common	Efficient retrieval, reduced duplication, better coordination
Cost and Infrastructure	Lower initial cost; high storage requirements	High setup cost; requires IT infrastructure
Scalability	Limited scalability	Highly scalable and adaptable
Ethical and Legal Issues	Limited tracking of consent and access	Complex issues of consent, ownership, and compliance
Overall Safety	Safer from cyber threats but weak in physical security	Safer when supported by strong cybersecurity and governance

GLOBAL PERSPECTIVES ON EHR PRIVACY AND DATA PROTECTION

The implementation and governance of electronic health records (EHRs) vary significantly across countries, reflecting differences in economic capacity, technological infrastructure, regulatory frameworks, and workforce readiness. Understanding these global variations is essential for identifying best practices and addressing gaps in safeguarding patient data and privacy.

High-Income Countries: High-income countries demonstrate advanced EHR implementation supported by strong regulatory frameworks, robust digital infrastructure, and substantial cybersecurity investments. These systems enable effective data governance, interoperability, and secure data exchange, reinforced by continuous workforce training[30].

Low- and Middle-Income Countries: Low- and middle-income countries face significant barriers, including infrastructure limitations, weak or inconsistent regulatory frameworks, workforce shortages, and financial constraints. These factors increase vulnerability to data breaches and hinder secure EHR implementation[31].

Lessons from International Practices: Global experience emphasizes the need for standardization, national digital health strategies, and harmonization of cross-border regulations. International collaboration is essential for developing secure, interoperable, and equitable EHR systems[32].

Legal, Ethical, and Policy Dimensions: EHR governance extends beyond technical safeguards, requiring integration of legal standards, ethical principles, and institutional accountability to address evolving challenges in digital healthcare[33].

Patient Confidentiality: Digital systems increase accessibility of data, elevating risks of unauthorized disclosure. Effective confidentiality depends on both technical safeguards and strict governance mechanisms[34].

Informed Consent in Digital Records: Informed consent is complex in digital contexts due to secondary data use. There is a need for dynamic, transparent consent models that support patient autonomy[35].

Data Ownership and Control: Ambiguity persists regarding ownership of health data. A shift toward patient-centered control is necessary to ensure ethical data governance and balanced decision-making[36].

Accountability of Healthcare Providers and Institutions: Audit trails enhance traceability; however, accountability is challenged by multi-stakeholder involvement. Clear roles and legal responsibilities are essential for effective enforcement[37].

- **Policy Frameworks and Governance:** Variations in policies and weak enforcement limit effective data protection. Strong, integrated legal and institutional frameworks are required to ensure secure and ethical use of EHR systems[38].

Overall, the legal, ethical, and policy dimensions of EHRs highlight the need for a multidimensional approach that integrates regulatory compliance, ethical responsibility, and institutional governance to ensure sustainable and secure use of digital health information.

EMERGING TECHNOLOGIES AND FUTURE SAFEGUARDS

The increasing complexity of cyber threats in digital healthcare necessitates advanced technologies to enhance the security and privacy of electronic health records (EHRs). While these technologies improve threat detection, data protection, and access control, their effectiveness depends on proper implementation, scalability, and alignment with ethical and regulatory frameworks[39].

- **Artificial Intelligence in Threat Detection:** AI enables anomaly detection and real-time monitoring, facilitating early identification of security threats. However, challenges include algorithmic bias, false positives, and dependence on high-quality data[40].
- **Blockchain for Health Data Security:** Blockchain ensures data integrity through decentralized and immutable records. Despite its advantages, limitations such as scalability issues, high computational cost, and integration complexity restrict widespread adoption[41].
- **Cloud Security Advancements:** Cloud technologies offer scalable storage with enhanced security features such as encryption and identity management. However, concerns related to data sovereignty, third-party dependence, and shared environment vulnerabilities persist[42].
- **Biometric Authentication:** Biometric systems improve authentication accuracy and reduce reliance on passwords. However, the sensitivity and non-replaceable nature of biometric data raise significant privacy and security concerns[43].
- **Zero-Trust Security Architecture:** Zero-trust models enforce continuous verification of users and devices, reducing unauthorized access risks. Implementation requires strong infrastructure, policy integration, and organizational commitment[44].

Overall, these technologies offer promising solutions for strengthening EHR security, but require careful integration with governance, regulation, and ethical considerations.

STRATEGIES TO STRENGTHEN EHR PRIVACY AND DATA SECURITY

Strengthening the privacy and security of electronic health records (EHRs) requires a comprehensive, multi-layered approach that integrates technical safeguards, organizational practices, and regulatory compliance. Effective strategies must address both technological vulnerabilities and human factors to ensure sustainable protection of patient data[45].

Strong Access Control Systems: Robust access control mechanisms are essential to limit data exposure. Role-based and attribute-based access controls should be implemented to ensure that users can access only the information necessary for their responsibilities. Multi-factor authentication, session timeouts, and least-privilege principles further enhance system security and reduce unauthorized access[46].

Regular Staff Training and Awareness: Human error remains a major contributor to data breaches. Continuous training programs are necessary to improve cybersecurity awareness among healthcare professionals. Training should focus on password management, phishing recognition, secure documentation practices, and adherence to privacy protocols, fostering a culture of data protection within institutions[47].

Periodic Security Audits: Regular security audits and risk assessments are critical for identifying vulnerabilities and ensuring compliance with established standards. Internal and external audits should evaluate system configurations, access logs, and data handling practices. Continuous monitoring enables early detection of anomalies and supports timely corrective actions[48].

Data Encryption and Secure Communication: Encryption of data at rest and in transit is a fundamental requirement for protecting sensitive health information. Secure communication protocols, including encrypted networks and secure messaging systems, prevent unauthorized interception of data. Strong cryptographic standards must be consistently applied and updated to address evolving threats[49].

Incident Response Planning: Healthcare organizations must establish structured incident response plans to manage data breaches and cybersecurity incidents

effectively. These plans should include procedures for detection, containment, mitigation, reporting, and recovery. Timely response minimizes damage, ensures continuity of care, and supports regulatory compliance[50].

- **Policy Development and Enforcement:** Comprehensive institutional policies are essential to guide secure data management practices. Policies should clearly define roles, responsibilities, and procedures related to data access, sharing, and protection. Strict enforcement, supported by accountability mechanisms, ensures adherence to privacy standards and legal requirements[51].
- **Patient Education and Digital Consent Models:** Empowering patients through education enhances transparency and trust in EHR systems. Patients should be informed about how their data are used, shared, and protected. Adoption of dynamic and digital consent models allows patients to exercise greater control over their information, supporting ethical data governance[52].
- **Vendor Accountability and Secure Interoperability Standards:** Third-party vendors and interoperable systems play a critical role in EHR ecosystems. Ensuring vendor accountability through contractual obligations, security certifications, and compliance standards is essential. Standardized and secure interoperability frameworks must be implemented to facilitate safe data exchange without compromising privacy[53].

Overall, the effectiveness of these strategies depends on their coordinated implementation across technical, organizational, and policy domains, ensuring a resilient and secure digital healthcare environment.

IMPLICATIONS FOR PRACTICE, EDUCATION, AND POLICY

- **Implications for Clinical Practice:** Healthcare professionals must adopt safe documentation practices and ensure strict confidentiality in handling digital records. Adherence to access control protocols, accurate data entry, and responsible information sharing are essential to minimize privacy breaches and enhance patient trust.
- **Implications for Nursing and Medical Education:** Integration of cybersecurity concepts into nursing and medical curricula is necessary to prepare healthcare professionals for digital practice environments. Emphasis on digital professionalism, ethical data handling, and awareness of privacy risks will strengthen competency in managing EHR systems.

Implications for Health Policy: Strengthening health policy frameworks is critical to ensure standardized and secure use of EHR systems. This includes the development of national standards, implementation of robust data protection legislation, and establishment of effective monitoring and accountability mechanisms to safeguard patient information.

CONCLUSION

Electronic health records (EHRs) have transformed healthcare by enhancing accessibility, continuity of care, and data management while offering significant advantages in safeguarding patient information through structured documentation, controlled access, and advanced security mechanisms. However, the digitization of health data also introduces complex vulnerabilities, including cybersecurity threats, ethical concerns, and governance challenges. Importantly, the effectiveness of EHRs in protecting patient privacy is not determined by technology alone. Robust outcomes depend on the integration of strong policy frameworks, continuous staff training, ethical practices, and effective governance systems. Emerging technologies provide additional opportunities to strengthen security, but their implementation must be supported by regulatory oversight and practical feasibility. A comprehensive, multi-dimensional approach that combines technological innovation with institutional accountability, user awareness, and policy enforcement is essential to ensure sustainable protection of patient data. Strengthening these components will be critical for building secure, trustworthy, and resilient digital healthcare systems.

Data Availability: No new data was generated or analyzed in this study. All information is derived from previously published literature.

Conflict of Interest: The authors declare no conflict of interest.

REFERENCES

- Ratwani RM. Electronic Health Records and Improved Patient Care: Opportunities for Applied Psychology. Current Directions in Psychological Science [Internet]. 2017 Aug 1;26(4):359–65. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC5553914/

- 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. Journal of Medical Internet Research [Internet]. 2022 Aug 24;24(9):e38144. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC9523524/
- Aldosari B. Cybersecurity in healthcare: new threat to patient safety. Cureus [Internet]. 2025 May 6;17(5):e83614. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC12141808/
- Ewoh P, Vartiainen T. Vulnerability to cyberattacks and Sociotechnical Solutions for health care Systems: Systematic review. Journal of Medical Internet Research [Internet]. 2024 Mar 8;26:e46904. Available from: https://doi.org/10.2196/46904
- Sachdeva S, Bhatia S, Harrasi AA, Shah YA, Anwer MdK, Philip AK, et al. Unraveling the role of cloud computing in health care system and biomedical sciences. Heliyon [Internet]. 2024 Apr 1;10(7):e29044. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC11004887/
- Conduah AK, Ofoe S, Siaw-Marfo D. Data privacy in healthcare: Global challenges and solutions. Digital Health [Internet]. 2025 May 1;11:20552076251343959. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC12138216/
- Baniulyte G, Rogerson N, Bowden J. Evolution – removing paper and digitising the hospital. Health and Technology [Internet]. 2023 Feb 22;13(2):263–71. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC9943586/
- Evans RS. Electronic health records: then, now, and in the future. Yearbook of Medical Informatics [Internet]. 2016 May 20;25(S 01):S48–61. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC5171496/
- Jayatissa P, Hewapathirana R. Enhancing Interoperability among Health Information Systems in Low and Middle-Income Countries: A Review of Challenges and Strategies. European Modern Studies Journal [Internet]. 2023 Aug 10;7(3):334–40. Available from: https://doi.org/10.59573/emsj.7(3).2023.31
- Zhang X, Saltman R. Impact of electronic health record interoperability on telehealth service outcomes. JMIR Medical Informatics [Internet]. 2021 Nov 14;10(1):e31837. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC8790688/
- 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. Informatics and Health [Internet]. 2024 Jun 13;1(2):123–48. Available from: https://doi.org/10.1016/j.infoh.2024.05.001
- Nowrozy R, Ahmed K, Kayes ASM, Wang H, McIntosh TR. Privacy Preservation of Electronic Health records in the Modern Era: A Systematic survey. ACM Computing Surveys [Internet]. 2024 Mar 19;56(8):1–37. Available from: https://doi.org/10.1145/3653297
- Grosman-Rimon L, Wegier P. With advancement in health technology comes great responsibility – Ethical and safety considerations for using digital health technology: A narrative review. Medicine [Internet]. 2024 Aug 16;103(33):e39136. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC11332755/
- Lyles CR, Nelson EC, Frampton S, Dykes PC, Cemballi AG, Sarkar U. Using electronic health record portals to improve patient engagement: Research priorities and best practices. Annals of Internal Medicine [Internet]. 2020 Jun 1;172(11_Supplement):S123–9. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC7800164/
- Abdelrahman E, Abdelrahim A, Mohamed T, Babikir M, Ahmed N, Gandour H, et al. Enhancing Clinical documentation: The effect of structured templates on Follow-Up notes in a Low-Resource hospital setting. Cureus [Internet]. 2025 Jul 22;17(7):e88510. Available from:

https://pmc.ncbi.nlm.nih.gov/articles/PMC12369448/

- Kannampallil T, Adler-Milstein J. Using electronic health record audit log data for research: insights from early efforts. Journal of the American Medical Informatics Association [Internet]. 2022 Sep 16;30(1):167–71. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC9748594/
- Basil NN, Ambe S, Ekhator C, Fonkem E. Health Records Database and Inherent Security Concerns: A Review of the literature. Cureus [Internet]. 2022 Oct 11;14(10):e30168. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC9647912/
- Shojaei P, Vlahu-Gjorgievska E, Chow YW. Security and Privacy of Technologies in Health Information Systems: A Systematic Literature review. Computers [Internet]. 2024 Jan 31;13(2):41. Available from: https://doi.org/10.3390/computers13020041
- Cobrado UN, Sharief S, Regahal NG, Zepka E, Mamauag M, Velasco LC. Access control solutions in electronic health record systems: A systematic review. Informatics in Medicine Unlocked [Internet]. 2024 Jan 1;49:101552. Available from: https://doi.org/10.1016/j.imu.2024.101552
- Pawelek J, Baca-Motes K, Pandit JA, Berk BB, Ramos E. The power of patient engagement with electronic health records as research participants. JMIR Medical Informatics [Internet]. 2022 Jun 21;10(7):e39145. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC9308075/
- Abughazalah M, Alsaggaf W, Saifuddin S, Sarhan S. Enhancing patient admission efficiency through a hybrid cloud framework for medical record sharing. Scientific Reports [Internet]. 2026 Jan 9;16(1):4926. Available from: https://www.nature.com/articles/s41598-026-35014-6
- Qureshi R, Koo I. A comprehensive survey of cybersecurity threats and data privacy issues in healthcare systems. Applied Sciences [Internet]. 2026 Feb 2;16(3):1511. Available from: https://doi.org/10.3390/app16031511
- Yeo LH, Banfield J. Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory analysis [Internet]. 2022. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC9123525/
- Ferreira JC, Elvas LB, Correia R, Mascarenhas M. Tokenization of electronic health records and healthcare data: enhancing security and privacy while enabling usability. Health and Technology [Internet]. 2025 Sep 17;15(6):1011–20. Available from: https://doi.org/10.1007/s12553-025-01012-3
- Alhuwail D, Al-Jafar E, Abdulsalam Y, AlDuaij S. Information security awareness and behaviors of health care professionals at public health care facilities. Applied Clinical Informatics [Internet]. 2021 Aug 1;12(04):924–32. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC8481013/
- Chuma KG. Legacy electronic health record systems as culprit behind cybersecurity risks in public healthcare facilities of South Africa. Global Security Health Science and Policy [Internet]. 2025 Jul 15;10(1). Available from: https://doi.org/10.1080/23779497.2025.2532556
- Moulaei K, Akhlaghpour S, Fatehi F. Patient consent for the secondary use of health data in artificial intelligence (AI) models: A scoping review. International Journal of Medical Informatics [Internet]. 2025 Mar 9;198:105872. Available from: https://doi.org/10.1016/j.ijmedinf.2025.105872
- Babatope AE, Adewumi IP, Ajisafe DO, Adepoju KO, Babatope AR. Assessing the factors militating against the effective implementation of electronic health records (EHR) in Nigeria. Scientific Reports [Internet]. 2024 Dec 28;14(1):31398. Available from: https://www.nature.com/articles/s41598-024-83009-y
- Stausberg J, Koch D, Ingenerf J, Betzler M. Comparing Paper-based with Electronic Patient Records: Lessons Learned during a Study on

Diagnosis and Procedure Codes. Journal of the American Medical Informatics Association [Internet]. 2003 Jun 10;10(5):470–7. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC212784/

- Raunaq FF, Islam S, Anam MdZ, Bari ABMM. Assessing the challenges to digital technology adoption in the healthcare sector: Implications for sustainability in emerging economies. Informatics and Health [Internet]. 2025 Sep 1;2(2):194–209. Available from: https://doi.org/10.1016/j.infoh.2025.09.001
- Olayiwola QB, Sanusi OM, Amoo GS, Agboola OJ, Adeyemi JA, Suleiman HA, et al. Barriers to digital health implementation in low- and middle-income countries: a narrative review. Discover Public Health [Internet]. 2026 Apr 12;23(1). Available from: https://doi.org/10.1186/s12982-026-01875-5
- Lee HA, Huang JC, Huang SW, Chen WH, Marcelo AB, Aljibe MSO, et al. Implementing a Cross-Border Next-Generation Personal Health Record in the Philippines and Taiwan: An Implementation case Report using Health Level 7 International Fast Healthcare Interoperability Resources. JMIR Formative Research [Internet]. 2025 May 2;9:e56272. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC12240210/
- Jain D. Regulation of digital healthcare in India: ethical and legal challenges. Healthcare [Internet]. 2023 Mar 21;11(6):911. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC10048681/
- Paul M, Maglaras L, Ferrag MA, Almomani I. Digitization of healthcare sector: A study on privacy and security concerns. ICT Express [Internet]. 2023 Feb 21;9(4):571–88. Available from: https://doi.org/10.1016/j.icte.2023.02.007
- Goldschmitt M, Gleim P, Mandelartz S, Kellmeyer P, Rigotti T. Digitalizing informed consent in healthcare: a scoping review. BMC Health Services Research [Internet]. 2025 Jul 2;25(1):893. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC12225439/
- Liddell K, Simon DA, Lucassen A. Patient data ownership: who owns your health? Journal of Law and the Biosciences [Internet]. 2021 May 26;8(2):lsab023. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC8487665/
- Fukami T. Enhancing healthcare accountability for administrators: fostering transparency for patient safety and quality enhancement. Cureus [Internet]. 2024 Aug 2;16(8):e66007. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC11366401/
- Mwogosi A, Simba R. Digital policy and governance frameworks for EHR systems in Tanzania: a scoping review. Digital Policy Regulation and Governance [Internet]. 2025 Apr 9;28(1):52–74. Available from: https://doi.org/10.1108/dprg-11-2024-0289
- Keshta I, Odeh A. Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal [Internet]. 2020 Aug 4;22(2):177–83. Available from: https://doi.org/10.1016/j.eij.2020.07.003
- Mohamed N. Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. Knowledge and Information Systems [Internet]. 2025 Apr 30;67(8):6969–7055. Available from: https://doi.org/10.1007/s10115-025-02429-y
- J A, Isravel DP, Sagayam KM, Bhushan B, Sei Y, Eunice J. Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. Journal of Network and Computer Applications [Internet]. 2023 Apr 3;215:103633. Available from: https://doi.org/10.1016/j.jnca.2023.103633
- Mehrtak M, SeyedAlinaghi S, MohsseniPour M, Noori T, Karimi A, Shamsabadi A, et al. Security challenges and solutions using healthcare cloud computing. Journal of Medicine and Life [Internet]. 2021 Aug 1;14(4):448–61. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC8485370/

- Nigam D, Patel SN, Vincent PMDR, Srinivasan K, Arunmozhi S. Biometric authentication for intelligent and Privacy-Preserving healthcare systems. Journal of Healthcare Engineering [Internet]. 2022 Mar 24;2022:1–15. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC8970854/
- Mushtaq S, Mohsin M, Mushtaq MM. A systematic literature review on the implementation and challenges of zero trust architecture across domains. Sensors [Internet]. 2025 Oct 3;25(19):6118. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC12526847/
- Kruse CS, Smith B, Vanderlinden H, Nealand A. Security techniques for the electronic health records. Journal of Medical Systems [Internet]. 2017 Jul 21;41(8):127. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC5522514/
- De Carvalho MA Junior, Bandiera-Paiva P. Health Information System Role-Based Access Control Current security Trends and Challenges. Journal of Healthcare Engineering [Internet]. 2018 Jan 1;2018:1–8. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC5836325/
- Clarke M, Martin K. Managing cybersecurity risk in healthcare settings. Healthcare Management Forum [Internet]. 2023 Aug 25;37(1):17–20. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC10725101/
- Hedda M, Malin BA, Yan C, Fabbri D. Evaluating the effectiveness of auditing rules for electronic health record systems [Internet]. 2018. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC5977720/
- Popoola O, Rodrigues MA, Marchang J, Shenfield A, Ikpehai A, Popoola J. An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security. Internet of Things [Internet]. 2024 Aug 3;27:101314. Available from: https://doi.org/10.1016/j.iot.2024.101314
- Jalali MS, Russell B, Razak S, Gordon WJ. EARS to cyber incidents in health care. Journal of the American Medical Informatics Association [Internet]. 2018 Oct 18;26(1):81–90. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC7647158/
- Almuballi BAS, Alshamlani MQN, Alghofaili YA, Alshammari FHL, Alattwei LMS, Alsaif AA, et al. Governance of clinical data quality in electronic health records: administrative policies, health informatics systems, and medical secretarial practices. International Journal of Computational and Experimental Science and Engineering [Internet]. 2024 Oct 30;10(4). Available from: https://doi.org/10.22399/ijcesen.4768
- Kassam I, Ilkina D, Kemp J, Roble H, Carter-Langford A, Shen N. Patient Perspectives and Preferences for Consent in the Digital Health Context: State-of-the-art Literature review. Journal of Medical Internet Research [Internet]. 2023 Jan 19;25:e42507. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC9960046/
- Ferreira JC, Elvas LB, Correia R, Mascarenhas M. Enhancing EHR Interoperability and Security through Distributed Ledger Technology: A Review. Healthcare [Internet]. 2024 Oct 2;12(19):1967. Available from: https://pmc.ncbi.nlm.nih.gov/articles/PMC11477175/