Data Privacy and Security Challenges In Electronic Health Records

Usman Mohammed[1], Mustapha Mukhtar Tijjani[2], Ridwan Salman[3]
[1, 2, 3]Bayero University Kano

I. BACKGROUND ON ELECTRONIC HEALTH RECORDS (EHRS)

Electronic Health Records (EHRs) are comprehensive digital repositories that store and manage patient health information for access by authorized healthcare providers. Over the past decade, healthcare systems have systematically adopted EHRs to improve the accessibility, accuracy, and interoperability of patient data. This digital transformation enhances clinical decision-making, strengthens evidence-based practice, and facilitates real-time patient monitoring and data exchange (Keshta & Odeh, 2021). With the proliferation of digital health infrastructures, concerns over privacy, data ownership, and security issues have intensified.
The integration of artificial intelligence (AI), cloud computing, and the Internet of Medical Things (IoMT) in healthcare has improved the usefulness and increased the vulnerability of electronic health record (EHR) systems. Recent studies indicate that while EHRs improve operational efficiency, they also increase the vulnerability to malicious actors (Folasole et al., 2023). The transition to linked health ecosystems necessitates robust frameworks to ensure the security, integrity, and availability of sensitive medical data across networks.

Importance of Data Privacy and Security in Healthcare

Data privacy and security are fundamental elements of ethical healthcare delivery. They ensure the safeguarding of confidential patient information from unauthorized access, exploitation, or revelation. In the context of EHRs, privacy refers to patients' rights to choose the use of their data, whereas security involves safeguarding such data from both external and internal threats (Keshta & Odeh, 2021). The importance of these features is underscored by international regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), which establish legal frameworks for the handling of personal health information.

A recent study emphasizes that privacy and security are not merely compliance requirements but essential for maintaining public trust in digital health services. Inadequate data protection can result in identity theft, insurance fraud, or harm to the reputation of healthcare institutions. Folasole et al. (2023) asserted that patient safety is fundamentally connected

to data security, as breaches can disrupt clinical workflows, delay care, and potentially endanger lives. Consequently, healthcare organizations are urged to adopt encryption, multifactor authentication, and blockchain-based integrity verification to bolster their defenses against breaches.

The increasing utilization of cloud-based storage and mobile EHR applications has shifted attention to distributed data governance. These platforms improve accessibility but challenge compliance by distributing data across jurisdictions with differing privacy standards (Keshta & Odeh, 2021). The growing digitization of healthcare has prompted the exploration of privacy-preserving computational techniques, such as federated learning and differential privacy, to balance data utility and protection.

Overview of Data Breaches and Cybersecurity Threats in Medical Systems

The incidence and complexity of cyberattacks on healthcare systems have markedly increased from 2021 to 2025. Healthcare data has emerged as a prime target for cybercriminals, with ransomware assaults, phishing, and insider threats being the prevalent means of intrusion. Global ransomware attacks like WannaCry and Ryuk underscored the susceptibility of hospital systems, resulting in the temporary cessation of essential medical services and the exposure of millions of patient records (Folasole et al., 2023).

Keshta and Odeh (2021) delineate five principal kinds of cybersecurity vulnerabilities impacting EHR systems, encompassing illegal access, malware penetration, inadequate authentication methods, and unsafe data transmission. In 2023, Folasole et al. discovered that a considerable number of healthcare businesses were deficient in advanced intrusion detection systems or real-time threat intelligence capabilities. Moreover, human error continues to be a significant risk factor—employees unintentionally compromise data through inadequate passwords, unprotected devices, or succumbing to phishing attacks.

Recent reports indicate emerging vulnerabilities, including data poisoning in AI-driven diagnostics and adversarial attacks on predictive health models (Folasole et al., 2023). These assaults jeopardize confidentiality and alter medical outcomes, demonstrating the intersection of cybersecurity and patient safety. As electronic health records develop into integrated ecosystems, cybersecurity frameworks must advance to incorporate AI-driven anomaly detection, zero-trust designs, and ongoing monitoring.

Research Problem Statement and Objectives

Despite significant advancements in technology and regulatory enforcement, healthcare companies continue to face data breaches that threaten patient confidentiality and institutional integrity. This study examines the growing gap between the implementation of electronic health records (EHR) and the development of appropriate privacy and security protocols. The healthcare sector's increasing dependence on digital platforms is impeded by numerous institutions' inadequate infrastructure, expertise, and financial resources to tackle complex cybersecurity threats (Keshta & Odeh, 2021; Folasole et al., 2023).

Research Objectives:

1. To identify and analyze the key data privacy and security challenges associated with Electronic Health Records (EHRs).
2. To assess the impact of cybersecurity threats on patient trust and healthcare delivery between 2021–2025.
3. To evaluate emerging technologies and frameworks that enhance EHR protection, such as blockchain, AI-based threat detection, and homomorphic encryption.
4. To propose practical recommendations for healthcare policymakers and IT administrators to mitigate privacy and security risks.

Scope and Significance of the Study

The ressearch investigates the privacy and cybersecurity issues associated with modern electronic health record systems employed in hospitals, clinics, and cloud-based medical platforms. The scope includes the analysis of technological vulnerabilities, institutional challenges, and the evolving regulatory landscape from 2021 to 2025. It employs modern literature to clarify the connection between data management, cybersecurity resilience, and patient safety. This work is crucial in advancing the global discourse on secure digital health ecosystems. As healthcare transforms into a data-driven field, understanding the balance between accessibility and security is crucial. This book provides healthcare professionals, policymakers, and system designers with insights to enhance EHR governance and compliance by highlighting contemporary research and case studies. Ultimately, addressing these privacy and security concerns will reduce operational and financial risks while bolstering patient confidence and engagement in the digital health transformation (Folasole et al., 2023).

II. LITERATURE REVIEW

1. Overview of Existing Research on Data Security and Privacy in EHRs

Recent study from 2021 to 2025 has highlighted the rapid development of data security protocols for Electronic Health Records (EHRs). The proliferation of healthcare digitization necessitates the urgent protection of sensitive medical information from unauthorized access and cyber threats. Osamika et al. (2025) conducted a thorough assessment that identified persistent shortcomings in EHR implementations, including the reliance on single-factor authentication and insufficient encryption methods (Osamika et al., 2025).

Nowrozy et al. (2024) emphasized that modern electronic health records (EHRs) are increasingly using privacy-preserving computation and blockchain technologies to ensure decentralized governance, immutability, and traceability of health records. These findings demonstrate that, despite global efforts for standardization, inconsistencies in data governance persist among healthcare organizations. Tawfik et al. (2025) argued that, despite the implementation of contemporary encryption methods, the absence of universal interoperability standards continues to pose hazards in data exchange.

Recent literature increasingly highlights AI-driven security analytics that employ predictive algorithms to detect anomalies and prevent breaches. However, concerns over algorithmic transparency and data equity impede its implementation (Gulkesen & Sonuvar, 2025). Recent studies jointly emphasize a paradigm shift towards "zero-trust" architectures that assume probable network breaches, necessitating continuous validation of identity and device integrity.

2. Common Frameworks, Standards, and Regulations (HIPAA, GDPR, and Beyond)

Data privacy and security in electronic health records are governed by legal and ethical frameworks that specify how healthcare institutions collect, process, and store personal health information. The Health Insurance Portability and Accountability Act (HIPAA) in the United States mandates administrative, physical, and technical safeguards for the protection of health data, while the General Data Protection Regulation (GDPR) in the European Union requires patient consent, data minimization, and the right to erasure.

Osamika et al. (2025) and Gulkesen & Sonuvar (2025) note that HIPAA and GDPR operate as complementary frameworks, with HIPAA focusing on healthcare entities and GDPR on individual autonomy. Emerging regulatory challenges with cross-border telemedicine and the cloud storage of health data require the establishment of multi-jurisdictional compliance solutions.

Nowrozy et al. (2024) highlighted that blockchain-based EHR systems intrinsically align with GDPR's principles of accountability and traceability; yet, the immutability of blockchain poses a barrier to the "right to be forgotten." Tawfik et al. (2025) presented "ACHealthChain," a blockchain-based access control framework that integrates GDPR-compliant privacy safeguards through dynamic consent and smart contracts.

The shift to federated health data models, particularly in Europe and North America, presents innovative compliance solutions that enable local retention of patient data while ensuring worldwide analyzability. This paradigm, while promising for vast medical research, introduces new concerns around metadata leakage and the guarantees of differential privacy (Pailkar & Murugan, 2025).

3. Review of Encryption, Authentication, and Access Control Methods

Encryption, authentication, and access control mechanisms are vital for the protection of electronic health records (EHR). Recent research underscores a shift from traditional symmetric encryption to hybrid and homomorphic encryption techniques, which enable processing of encrypted data without the need for decryption (Vyavahare, 2025). These technologies ensure that, even if unauthorized individuals access the storage media, the data remains unintelligible.

Cryptography

Pandey et al. (2025) introduced multi-layered cryptographic techniques that combine elliptic curve cryptography (ECC) with AES algorithms to protect electronic health record (EHR) data during transmission and storage. Nedunoori (2025) investigated IoT-based healthcare encryption, emphasizing quantum-resistant encryption methods to protect data from post-quantum vulnerabilities. Hybrid encryption, which combines symmetric and asymmetric techniques, has shown an effective equilibrium between computational efficiency and security strength (Vyavahare, 2025).

Identity verification

Authentication remains a critical vulnerability in healthcare cybersecurity. Single-factor authentication, particularly passwords, is sometimes regarded as insufficient. The propensity for biometric authentication techniques, including facial recognition, fingerprint analysis, and ECG-based identity verification, is increasing, as evidenced by Osamika et al. (2025). Furthermore, multi-factor authentication (MFA) utilizing time-based one-time passwords (TOTPs) and hardware tokens has become the recommended standard.

Access Regulation

Access control frameworks specify the authorization for information access inside EHR systems. Chakravarthy et al. (2025) presented a hybrid blockchain-hashing access control method that enables real-time permission verification and ensures tamper-proof audit trails. Tawfik et al. (2025) enhanced this concept through attribute-based encryption (ABE) and smart-contract governance, enabling meticulous regulation of patient data transmission while maintaining anonymity.

Furthermore, Nowrozy et al. (2024) investigated role-based access control (RBAC) and context-aware dynamic access control, which modify authorization levels based on user location, time, and operational context. Adaptive models are more vital as healthcare systems integrate IoT devices, mobile applications, and cloud-based platforms.

4. Summary of Identified Gaps and Unresolved Challenges

Notwithstanding considerable progress, substantial deficiencies persist in guaranteeing comprehensive data privacy and security in EHR systems.

The fourth aspect pertains to standardization and interoperability.

While interoperability facilitates coordinated treatment, it simultaneously amplifies the number of potential attack routes. Research indicates a lack of uniformly applied security standards across all platforms. Various encryption methodologies and access patterns hinder electronic health record (EHR) providers from transmitting data seamlessly (Nowrozy et al., 2024).

Scalability of Blockchain Technology-Based Systems at 4.2

Although blockchain frameworks such as those developed by Chakravarthy et al. (2025) and Tawfik et al. (2025) enhance transparency and integrity, significant limitations regarding scalability and latency persist. These solutions sometimes require substantial computational resources and face difficulties in integrating with legacy EHR systems.

Discrepancies in Regulatory Policies 4.3

Gulkesen and Sonuvar (2025) assert that global data sharing is impeded by legal inconsistencies and contradictions among HIPAA, GDPR, and emerging privacy regulations in regions such as Asia and Africa. The immutability dilemma of the General Data Protection Regulation (GDPR), which entails reconciling data erasure rights with the permanence of blockchain technology, persists in presenting issues for compliance officers.

Users' Awareness and the Impact of Human Factors

A major issue that persists in causing data breaches is human error. Osamika et al. (2025) identified inadequate cybersecurity training and deficient password hygiene as two prevalent causes of unauthorized access incidents. The establishment of thorough cybersecurity education and policy inside healthcare companies is essential to mitigate these problems.

Ethics in Artificial Intelligence and Privacy-Enhancing Analytics

The prevalence of challenges related to data bias, model transparency, and re-identification risks has escalated as artificial intelligence increasingly integrates into predictive diagnoses and clinical decision support. Pailkar and Murugan (2025) assert that federated learning systems, despite their many benefits, are susceptible to inference attacks that may expose confidential patient data.

5. Synthesis and Future Research Directions

Encryption, blockchain technology, and artificial intelligence offer opportunities for the advancement of electronic health record (EHR) security. Future research must focus on creating lightweight cryptographic algorithms for mobile devices, federated artificial intelligence that safeguards user privacy, and quantum-resistant key exchange protocols. Interdisciplinary collaboration among physicians, technologists, and policymakers is essential for the development of resilient, compliant, and patient-centered digital health ecosystems.

Chakravarthy et al. (2025) and Nowrozy et al. (2024) exemplify current studies proposing hybrid systems that integrate the immutability of blockchain technology with AI-driven anomaly detection. These hybrid methodologies would yield an adaptable cybersecurity framework for the healthcare sector. The future of safe digital health infrastructure will hinge on the effective resolution of scalability, governance, and usability challenges.

Methodology

Research Methodology This study utilizes a Systematic Literature Review (SLR) technique to qualitatively evaluate the status of data privacy and security in Electronic Health Record (EHR) systems. The review emphasizes the synthesis of secondary data to discern patterns, technological deficiencies, and emerging solutions in healthcare cybersecurity.

Data Sources and Search Methodology A thorough search was performed across academic databases such as IEEE Xplore, PubMed, ScienceDirect, and Google Scholar. The search employed terms including "EHR Security,""Healthcare Privacy Challenges,""Blockchain in Healthcare," and "AI in Data Security."

Inclusion and Exclusion Standards The study employed the subsequent criteria to maintain relevance and timeliness:

Inclusion criteria: Peer-reviewed journal publications, conference proceedings, and credible industry reports published from 2021 to 2025. Submissions must explicitly focus on the technical or regulatory dimensions of EHR security.

Exclusion criteria: Articles published before 2021, non-English publications, and opinion pieces devoid of empirical or theoretical substantiation.

Data Examination Papers were classified according to three topical pillars: (1) Current Threat Landscapes, (2) Regulatory Compliance Gaps, and (3) Technological Mitigation Strategies. This theme analysis facilitated the triangulation of findings across various healthcare contexts and jurisdictions. The effectiveness of these frameworks is evaluated concerning the CIA triad—Confidentiality, Integrity, and Availability—alongside metrics for latency, scalability, and compliance with standards such as ISO/IEC 27001, ensuring a thorough assessment of both technical efficacy and operational readiness in healthcare environments (Asimiyu, 2025; Prosper, 2025).

III. RESULTS / FINDINGS

1. Analysis of the Most Significant Data Privacy and Security Challenges

The analysis revealed that the principal challenges facing Electronic Health Records (EHRs) from 2021 to 2025 involve ransomware attacks, unauthorized access, shortcomings in data interoperability, and vulnerabilities in cloud infrastructure. Osamika et al. (2025) found that more than 70% of healthcare facilities globally still rely on obsolete authentication mechanisms and insufficient encryption, making systems susceptible to insider threats and phishing assaults (Osamika et al., 2025). Rani et al. (2025) similarly identified significant shortcomings in the implementation of national EHR security mandates, particularly in low- and middle-income nations where resource constraints impede compliance with GDPR and HIPAA rules (Rani et al., 2025).

A persistent issue is the dependence on third-party providers for cloud storage, which poses multi-tenancy risks and potential data leakage vulnerabilities (Oyekunle & Tiwo, 2025). Inadequate network segmentation, insufficient access control protocols, and lack of endpoint encryption are commonly recognized structural vulnerabilities that result in breaches.

2. Trends in Cyber Threats Affecting EHR Systems

Recent research reveal a substantial rise in ransomware and phishing attacks targeting healthcare data. Xu (2025) reported a 45% increase in healthcare breaches in the United States from 2020 to 2024, attributing this surge to the growing digitalization of patient records and the integration of Internet of Medical Things (IoMT) devices (Xu, 2025). Yankson et al. (2025) analyzed 145 healthcare breach incidents in the U.S. and found that 68% were attributable to hacking, with ransomware being the primary attack vector.

Makinde (2025) highlighted the growing intricacy of social engineering attacks and deepfake identity impersonation, which exploit human fallibility and insufficient authentication to get access to electronic health records (Makinde, 2025). The evolution of these attacks underscores the shift from opportunistic cybercrime to intentional assaults on healthcare data assets, often driven by financial incentives and espionage.

Zarkia and Usman (2025) asserted that healthcare networks integrated with the IoT represent an increasing domain of vulnerability, as unsecured biomedical sensors and wearable devices expose endpoints that can be exploited for lateral movement into electronic health record databases (Zarkia & Usman, 2025).

3. Case Studies and Examples

3.1. Case Study 1 – Ransomware in Cloud-Based EHR Systems

Oyekunle and Tiwo (2025) analyzed a simulated ransomware incident utilizing the NIST and MITRE ATT&CK frameworks, demonstrating that healthcare organizations reliant on hybrid cloud infrastructures were disproportionately affected by supply chain attacks and cloud misconfigurations. Their model demonstrated that the use of multilayer security, which includes behavior-based intrusion detection and automatic rollback capabilities, reduced recovery time by 42% (Oyekunle & Tiwo, 2025).

3.2. Case Study 2 – Breach Trends in Integrated EHR Systems

Yankson et al. (2025) documented numerous substantial data breaches occurring from 2021 to 2023, including an event in which an integrated EHR network was compromised, affecting 3 million patient records due to insecure APIs connecting hospital systems. Mitigation involved zero-trust network segmentation and continuous threat monitoring, leading to a 60% decrease in breach recurrence rates.

3.3. Case Study 3 – Implementation Gaps in National EHR Standards

Rani et al. (2025) conducted a nationwide implementation gap analysis in Indonesian healthcare facilities, revealing that just 40% employed effective encryption technologies and less than 30% undertook annual cybersecurity audits. The results highlight the disparity between policy and execution in data security in impoverished nations.

4. Review of Simulation and Model Performance

The literature review analyzed various simulation studies to assess the effectiveness of emerging security technologies.

Outcomes of Blockchain Implementation: Research employing Hyperledger Fabric repeatedly indicates that blockchain-based access control improves data integrity. Research indicates that these systems can offer immutable transaction logging and verifiable audit trails, with certain models attaining near real-time detection of unauthorized change attempts (Chakravarthy et al., 2025).

The examination of AI-driven security frameworks underscores the effectiveness of federated machine learning in anomaly detection. Makinde (2025) indicated that these models might achieve precision rates of up to 96.7% in detecting intrusion attempts in remote EHR environments while maintaining patient data confidentiality.

Hybrid Encryption Performance: Comparative examinations of encryption standards indicate that the integration of AES-256 with Elliptic Curve Cryptography (ECC) markedly enhances data confidentiality relative to conventional symmetric encryption. Vyavahare (2025) observed that these intensified security protocols typically lead to a marginal increase in transactional latency, averaging 0.9 seconds per transaction, representing a trade-off for improved security.

Overall Assessment: The consensus across reviewed simulations indicates that integrating AI-driven monitoring with blockchain-backed audit trails provides the most balanced defense against modern EHR threats. Nonetheless, scalability and computational demands remain critical constraints identified in the literature.

IV. DISCUSSION

1. Interpretation of Findings in Context of Existing Literature

This research highlights the consensus in recent studies (2021–2025) that Electronic Health Records (EHRs) face a complex range of data privacy and security threats that surpass traditional legal frameworks such as HIPAA and GDPR. While these frameworks provide structural underpinnings for data security, they insufficiently tackle AI-driven attacks, blockchain vulnerabilities, and IoT-related threats (Ali, 2025; Vadisetty & Polamarasetti, 2025). The empirical evidence indicates an increase in ransomware instances and unauthorized access, along with prior systematic evaluations that identified phishing, misconfigured cloud storage, and third-party integrations as major threat vectors (Osamika et al., 2025). The simulations demonstrating enhanced effectiveness of AI-enhanced anomaly detection and blockchain audit trails support the theoretical claim made by Kumar (2025), which argues that multi-layered, hybrid architectures exceed standalone cryptographic systems in safeguarding digital health infrastructures. These findings correspond with Hussain (2025), who emphasized the imperative for healthcare systems to transition from reactive to proactive security methods, incorporating real-time data analytics, federated learning, and zero-trust frameworks to avert assaults before breaches occur. Notwithstanding technological progress, organizational culture and policy enforcement remain essential, as more than 60% of data breaches arise from human error or ignorance (Kięczkowska, 2025).

2. Implications for Healthcare Providers, Patients, and Policymakers

For Medical Practitioners

Healthcare businesses must reframe cybersecurity as a critical concern for clinical safety rather than merely a compliance issue. The findings demonstrate that continuous threat monitoring, multi-factor authentication, and encryption standardization are crucial for preserving patient trust. Vadisetty and Polamarasetti (2025) observed that hospitals employing the Health Industry Cybersecurity Practices (HICP) framework realized measurable reductions in security incidents by integrating technological defenses with organizational controls. Furthermore, worker training and cybersecurity awareness are crucial, particularly given the growing complexity of medical IoT environments (Kięczkowska, 2025).

For Patients

Patients, as data subjects, are more susceptible to threats like as identity theft, data commodification, and medical fraud. The research highlights the importance of patient-focused security protocols that enhance transparency and control. Ali (2025) proposes "digital consent dashboards" that allow patients to dynamically review, authorize, or revoke access to their records, in accordance with GDPR's right to access and right to erasure principles.

For Executives

The research emphasizes the need for interoperable and technology-neutral regulations that align national standards with global frameworks like GDPR and HIPAA. Chen and Wald (2025) contend that existing regulations were not designed to incorporate technologies such as blockchain, artificial intelligence, or cross-border data analytics. Consequently, upcoming regulations should incorporate AI auditing methodologies, blockchain compliance structures, and automated policy enforcement tools that provide traceability and accountability in digital health transactions.

3. Evaluation of Current Privacy Frameworks and Their Limitations

The comparative analysis of HIPAA and GDPR reveals inherent limitations in their relevance to decentralized and cloud-based healthcare environments. While HIPAA has comprehensive administrative and physical precautions, it lacks effective real-time breach detection, accountability for artificial intelligence, and regulations for international data transfers (Vadisetty & Polamarasetti, 2025). In contrast, GDPR promotes patient autonomy and data minimization but encounters the immutability paradox—the difficulty of reconciling the "right to be forgotten" with the permanent ledger framework of blockchain (Ikhalea et al., 2025).

Moreover, enforcement is irregular. Osamika et al. (2025) note that regulatory compliance often prioritizes documentation above measurable cybersecurity performance. This has created a compliance-security dilemma where institutions follow regulatory standards but nevertheless face significant vulnerabilities. The HICP model, created by U.S. authorities, aims to rectify this shortcoming by combining technical safeguards (such as endpoint protection) with behavioral risk management (including phishing simulation training); nonetheless, global acceptability remains variable.
Furthermore, Ali (2025) and Kumar (2025) assert that emerging threats, such as adversarial AI attacks and quantum decryption, require the continual adaptation of existing systems. Without scalable compliance integration, privacy standards risk becoming obsolete as healthcare data management evolves towards decentralized, AI-augmented systems.

4. Recommendations for Improving EHR Data Protection

Based on the results and reviewed literature, several strategic recommendations are proposed:

1. Implement AI-Enhanced Cyber Defense Systems: Healthcare providers should employ machine learning-based anomaly detection and automated intrusion response mechanisms to enhance traditional firewalls and encryption techniques. Research by Ikhalea et al. (2025) indicates that AI-integrated blockchain frameworks can enhance threat detection accuracy by over 90%.
2. Implement Blockchain-Enabled Auditability: Blockchain-based EHR platforms can ensure data integrity and non-repudiation by maintaining immutable records of access and alterations. Hybrid approaches must be employed to enable selective data erasure for GDPR compliance (Kumar, 2025; Asha et al., 2025).
3. Augment Data Governance and Compliance measures: Policymakers should shift from static regulatory checklists to dynamic, risk-based compliance measures. The implementation of smart contracts for automated HIPAA/GDPR verification may significantly reduce human error and improve audit efficiency (Vadisetty & Polamarasetti, 2025).
4. Promote Global Interoperability Standards: The international harmonization of EHR security protocols is vital. The implementation of multi-stakeholder frameworks such as ISO/IEC 27701 and FHIR-based data exchange is crucial for enhancing cross-border data sharing while ensuring privacy protection.
5. Invest in Workforce Training and Awareness: Ongoing cybersecurity education should be obligatory throughout healthcare sectors. Kięczkowska (2025) asserts that staff training and accountability are the most cost-effective strategies for managing insider risks.
6. Advocate for Research in Quantum-Safe Cryptography: As quantum computing advances, traditional encryption methods face the threat of obsolescence. Prioritizing the continuous research and development of quantum-resistant algorithms is crucial for safeguarding the future security of electronic health record systems.

In conclusion, safeguarding EHRs requires an **ecosystem approach** that combines robust legal frameworks, adaptive technologies, and continuous stakeholder education. The integration of blockchain, AI, and regulatory innovation promises a secure and ethical path forward in digital healthcare transformation.

REFERENCES

[1] Aghaunor, C. T., Eshua, P., & Obah, T. (2025). *Data security strategies to avoid data breaches in modern information systems.*ResearchGate.

[2] Ali, A. (2025). *Ethics, Privacy, and Security.*Google Books.

[3] Arefin, N. T. Z. S. (2025). Future-Proofing Healthcare: The Role of AI and Blockchain in Data Security.

[4] Asha, A. I., Arafat, M. D. S., Desai, K., & Hossain, M. A. (2025). *The role of blockchain and AI in revolutionizing electronic health records: A business-driven approach to data security and interoperability.*IIBA Journal.

[5] Asimiyu, Z. (2025). Privacy-Preserving Machine Learning in Healthcare: Balancing Data Sharing, AI, and Patient Confidentiality. [ResearchGate](https://www.researchgate.net/publication/396371995_Privacy-Preserving_Machine_Learning_in_Healthcare_Balancing_Data_Sharing_AI_and_Patient_Confidentiality).

[6] Chakravarthy, D. G., Gopi, R., Murugan, S., & Joseph, E. R. (2025). *Enhancing confidentiality and access control in electronic health record systems using a hybrid hashing blockchain framework.*Nature Scientific Reports.

[7] Chen, P. H., & Wald, C. (2025). *A review of cybersecurity and privacy standards in medical imaging: Consensus, frameworks, and best practices.*ScienceDirect.

[8] Folasole, A., Adegboye, O. S., & Ekuewa, O. I. (2023). *Security, privacy challenges and available countermeasures in electronic health record systems: A review.*EJECE Journal.

[9] Gulkesen, K. H., & Sonuvar, E. T. (2025). *Data Privacy in Medical Informatics and Electronic Health Records: A Bibliometric Analysis.*Springer.

[10] Hussain, I. (2025). *Securing healthcare in the age of AI: A comprehensive review of cybersecurity challenges and solutions.*Global Research Review.

[11] Ikhalea, N., Chianumba, E. C., Mustapha, A. Y., & Forkuo, A. Y. (2025). *A conceptual framework for enhancing healthcare data security using blockchain and AI.*ResearchGate.

[12] Keshta, I., & Odeh, A. (2021). *Security and privacy of electronic health records: Concerns and challenges.*ScienceDirect.

[13] Kięczkowska, J. (2025). *Securing medical applications: Best practices for protecting data from cyber threats.*Biblioteka Nauki.

[14] Kumar, P. (2025). *Securing digital-first healthcare: AI, blockchain, and cloud architectures for personal health data protection.*IJAM Journal.

[15] Makinde, O. F. (2025). *Navigating cyber threats in health information systems: Safeguarding patient and clinical data.*ResearchGate.

[16] Nedunoori, V. (2025). *A Comprehensive Review of Encryption and Protection Techniques for Healthcare Data.*Springer. PhilPapers](https://philpapers.org/rec/SABFHT-2).

[17] Nowrozy, R., Ahmed, K., Kayes, A. S. M., & Wang, H. (2024). *Privacy preservation of electronic health records in the modern era: A systematic survey.*ACM Digital Library.

[18] Osamika, D., Adelusi, B. S., & Kelvin-Agwu, M. T. C. (2025). *A Systematic Review of Security, Privacy, and Compliance Challenges in Electronic Health Records: Current Practices and Future Directions.*ResearchGate.

[19] Osamika, D., Adelusi, B. S., & Kelvin-Agwu, M. T. C. (2025). *A systematic review of security, privacy, and compliance challenges in electronic health records.*ResearchGate.

[20] Oyekunle, S. M., & Tiwo, O. J. (2025). *Enhancing data resilience in cloud-based electronic health records through ransomware mitigation strategies using NIST and MITRE ATT&CK frameworks.*ResearchGate.

[21] Pailkar, H., & Murugan, T. (2025). *A Literature Study on Blockchain-Based Access Control for Electronic Health Records.*Taylor & Francis.

[22] Pandey, S., Bhushan, B., & Obaid, A. J. (2025). *Improving Data Security and Privacy in Health Care: Cryptographic Techniques and Security Protocols.*Springer.

[23] Prosper, J. (2025). Modern Encryption Techniques, Blockchain, and AI in Action: A Multi-Sectoral Study on Securing Healthcare, Mobile Applications, Databases, and Smart Cities.

[24] Rani, D. M., Mayasari, W., Faraswati, R., & Luni, D. (2025). *Implementation gap analysis of national electronic health record (EHR) data security standards in primary healthcare facilities.*GPI Journal.

[25] Rathore, N., Kumari, A., & Patel, M. (2025). Synergy of AI and Blockchain to Secure Electronic Healthcare Records. [Wiley Online Library](https://onlinelibrary.wiley.com/doi/abs/10.1002/spy2.463).

[26] Taherdoost, H. (2025). Blockchain for Security and Privacy in the Smart Healthcare. [ScienceDirect](https://www.sciencedirect.com/science/article/pii/B9780443363702000190).

[27] Tawfik, A. M., Al-Ahwal, A., Eldien, A. S. T., & Zayed, H. H. (2025). *Blockchain-based access control and privacy preservation in healthcare: A comprehensive survey.*SpringerLink.

[28] Truong, T. (2025). The Research on the Application of Blockchain Technology in the Security of Digital Healthcare Data. [Scholar Press](http://scholar-press.com/uploads/papers/DbUMWrR9cBW29WLecihBWsVdWID2iD344nwKuOtG.pdf).

[29] Vadisetty, R., & Polamarasetti, A. (2025). *Regulatory framework for digital health, data privacy, and cybersecurity.*Taylor & Francis.

[30] Vyavahare, R. R. (2025). *Exploring Hybrid Encryption for Enhanced Security of Electronic Health Record in Cloud Environment.*Norma Institutional Repository.

[31] Xu, L. (2025). *Trends in US healthcare data breaches.*IEEE Xplore.

[32] Yankson, B., Barati, M., Bondzie, R., & Madani, R. (2025). *The rise of hacking in integrated EHR systems: A trend analysis of US healthcare data breaches.*MDPI.

[33] Zarkia, M. N. H., & Usman, S. (2025). *IoT data breaches and privacy issues in healthcare systems.*Oiji Journal.