Sarcouncil Journal of Engineering and Computer Sciences

ISSN(Online): 2945-3585

Volume- 04| Issue- 12| 2025

Research Article **Received:** 25-10-2025| **Accepted:** 20-11-2025 | **Published:** 03-12-2025

Protecting Electronic Health Records (EHRs): Advances and Challenges in Data Security and Privacy

***Abimbola Filani*[1], *and Jochebed Akoto Opoku*[2]**

[1]*Department of Business Information Systems, Central Michigan University, Michigan, USA*
[2]*Department of Telecommunication Engineering, Kwame Nkrumah University of Science and Technology, Ghana*

Abstract: The widespread use of Electronic Health Records (EHRs) has improved healthcare delivery, enhancing data access, clinical decision-making, and care coordination. However, this digital shift has created new challenges in protecting patient data from cyber threats, unauthorized access, and privacy concerns. This research critically evaluates the changing environment of EHR security, focusing on important vulnerabilities such as ransomware, insider misuse, and interoperability issues. It investigates cutting-edge technology solutions such as enhanced encryption, blockchain, artificial intelligence, and biometric authentication that aim to protect data integrity, confidentiality, and availability. It also addresses the ethical and legislative aspects of privacy preservation, highlighting the importance of patient permission and worldwide data protection systems. Despite tremendous advances, ongoing challenges posed by legacy systems, high installation costs, and human error continue to jeopardize EHR security. This paper also proposed recommendations for future directions in developing robust, patient-centric digital health ecosystems.

Keywords: Electronic Health Records, Data Breaches, Data Privacy, Regulatory Compliance.

INTRODUCTION

Electronic Health Records (EHRs) are digital versions of paper charts that healthcare providers and hospitals have long kept for each patient (Igwama *et al.*, 2024). The idea of maintaining patient information electronically began with simple databases for laboratory results and billing. Over the last 30 years, it has evolved into complete systems that incorporate a wide range of patient data, such as demographics, medical history, test results, prescriptions, and treatment plans. All this information is housed on a single, easily accessible digital platform. The global push for digital transformation in healthcare, particularly through government-led initiatives and incentive programs, increased EHR adoption in the early 2000s (Shen, Y., *et al.*, 2025). These endeavors sought to replace messy paper-based systems with more efficient, interoperable, and secure electronic records. The ultimate goal was to help clinicians make better decisions and improve care coordination (Keshta & Odeh, 2021).

In today's healthcare sector, EHRs have become the foundation of modern clinical practice. They improve patient information availability while reducing diagnostic test duplication. These technologies also improve overall care quality by providing healthcare practitioners with fast access to up-to-date information. EHRs promote continuity of care, reduce medication mistakes, and enable evidence-based decision-making. Furthermore, they help to achieve broader public health goals by facilitating health data analytics for disease surveillance, healthcare planning, and medical research. Simply put, an EHR is a secure online file for each patient that may be shared with approved clinicians, pharmacies, laboratories, and insurers. This enables seamless communication and collaboration, something paper records could never do (Mohammad, A. A. S., et al, 2025).

However, the digital transformation of healthcare has created various additional challenges. As EHR systems rely more on cloud computing, mobile applications, and networked data interchange, the risk of illegal access, data breaches, and cyberattacks increases. Insider misuse, ransomware, and data interception during transmission are some of its common dangers (Igwama *et al.*, 2024). Insider misuse happens when hospital personnel or clinicians gain unlawful access to patient information, violating confidentiality. Ransomware attacks, in which hackers encrypt hospital data and demand payment to decrypt it, have become a big worry (Jiang *et al.*, 2025). In some circumstances, these attacks have led healthcare facilities to shut down systems and delay patient care. Data stored or processed in third-party cloud environments may potentially be vulnerable if proper encryption, authentication, and auditing measures are not in place (Bani Issa *et al.*, 2020).

Apart from technical weaknesses, human and organizational factors represent substantial risks. Inadequate staff training, weak password rules, lack of role-based access control, and ambiguous

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

***Corresponding Author:** Jochebed Akoto Opoku

DOI- https://doi.org/10.5281/zenodo.17806051

data-handling protocols all lead to security flaws. According to studies by Mohammad et al. (2025), many frontline healthcare professionals are still apprehensive about EHR systems' reliability and privacy. They are concerned that illegal access or system failures could jeopardize patient safety. These non-technical factors, such as insufficient policy enforcement and cybersecurity knowledge, frequently have a significant impact on how effectively EHR systems protect patient data (Mohammad *et al.*, 2025).

EHR security involves more than just sophisticated software. It requires a careful balance of confidentiality, integrity, and availability, which are the three fundamental principles of information security. Confidentiality ensures that only authorized personnel have access to sensitive information. Integrity ensures that data is accurate and unaffected. Availability ensures that authorized users have access to information when they need it (Mohammad, *et al*., 2025). Failure to follow any of these principles can have major clinical and ethical ramifications. For example, if an EHR system fails during an emergency, clinicians may be unable to obtain important allergy information, potentially jeopardizing a patient's life. Similarly, if a record is edited maliciously or inadvertently, it may result in incorrect treatments or misdiagnoses (Lee, L. M., 2017).

OVERVIEW OF ELECTRONIC HEALTH RECORDS (EHRS)

Electronic health records (EHRs) are computerized systems that gather, store, and manage patients' medical information in healthcare settings. They contain information such as patient demographics, medical histories, laboratory test results, imaging data, medications, allergies, and treatment plans (Igwama *et al.*, 2024). Essentially, an EHR is a secure, regularly updated digital chart that authorized clinicians and personnel can view from multiple institutions. This technology allows healthcare workers to better coordinate care, evaluate outcomes, and decrease test and procedure duplication (Häyrinen & Nykänen, 2008).

Globally, EHR usage has risen dramatically during the last two decades. In the United States, national policy measures such as the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 sped up deployment by providing financial incentives to hospitals and clinics that proved "meaningful use" of digital records (Anzalone *et al.*, 2025) Over 95% of hospitals in the United States and around 90% of office-based physicians were predicted to have implemented approved EHR systems in 2021. The United States has significantly increased EHR adoption to improve healthcare efficiency and accessibility. For instance, following the implementation of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, U.S. hospitals and clinics rapidly adopted certified EHR systems. A national survey of over 2,000 family physicians revealed that more than 60% reported being satisfied with their EHR systems, particularly when usability features were well-designed and supported by efficiency strategies such as voice recognition and templated text (Schwappach *et al.*, 2024).

EHRs provide significant benefits in clinical care, research, and public health. Clinically, they aid decision-making by alerting doctors to potential pharmaceutical interactions or allergies, hence enhancing diagnostic accuracy and care coordination. For researchers, EHR data provides enormous databases for epidemiological and clinical studies. Public health officials use aggregated EHR data to track disease outbreaks, assess health trends, and plan interventions (Igwama *et al.*, 2024). However, these benefits are contingent on preserving trust in data security, privacy, and integrity. For example, imagine your doctor had fast access to your medical history, prescriptions, and test results on a computer, eliminating the need to repeat the same test or remember all the facts. That is the convenience of an EHR. However, this accessibility must be accompanied by security measures to ensure that hackers or unauthorized others do not gain access to confidential information (McDermott *et al.*, 2019).

Table 1. Advantages vs. Risks of EHR Adoption (Tsai, *et al.*, 2020)

Advantages	**Potential Risks**
Quick and easy access to patient records across departments and facilities	Unauthorized access by internal staff or hackers
Reduced medical errors through clinical alerts and automated checks	Data breaches exposing sensitive patient information
Enhanced coordination among healthcare providers	System failures leading to downtime or loss of

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

	data
Improves billing accuracy and administrative efficiency	Dependence on third-party vendors with possible vulnerabilities

DATA SECURITY AND PRIVACY RISKS IN ELECTRONIC HEALTH RECORDS (EHRS)

The use of Electronic Health Records (EHRs) has altered healthcare delivery by increasing accessibility, coordination, and efficiency. However, this change has added a new layer of risk, one focused on data security and patient privacy. As EHR systems become increasingly connected to cloud platforms, mobile applications, and external networks, they become vulnerable to a range of cyber, organizational, and human vulnerabilities. Protecting patient information has thus become one of the most pressing issues in modern healthcare (Keshta & Odeh, 2021).

Cybersecurity Threats

Cybersecurity attacks are the most immediate and obvious threat to EHR systems. These dangers leverage both technological flaws and human error. Malware, ransomware, phishing, and insider misuse are among the most alarming, as they all have the potential to significantly disrupt healthcare operations. Malware and ransomware attacks have grown increasingly common in the healthcare sector. These attacks often involve malicious malware accessing hospital networks through compromised emails, downloads, or network flaws. Once triggered, ransomware encrypts sensitive patient information and demands payment to restore access. Hospitals that fall victim to such attacks frequently endure complete operational shutdowns, delayed treatments, and significant financial losses (Jiang *et al.*, 2025). For example, the 2020 ransomware attack on Düsseldorf University Hospital in Germany prompted the hospital to move patients to other institutions, resulting in at least one patient death from delayed care. Such cases demonstrate how cybersecurity flaws in EHR systems go beyond financial or reputational damage and risk patient lives directly (Ewoh & Vartiainen, 2024).

Phishing attacks are another widespread issue. In these assaults, cybercriminals send fake emails that look to be real, luring healthcare personnel into disclosing passwords or clicking on malicious links. Because medical professionals are frequently under time constraints, phishing emails can readily elude vigilance (Tiwo *et al.*, 2025). A single hijacked email account can provide attackers access to thousands of patient records, as happened in multiple US hospitals between 2020 and 2022 (Osifowokan *et al.*, 2025). Insider threats, whether intentional or inadvertent, pose significant hazards. Employees with authorized access to EHRs may mishandle data, divulge sensitive information, or fall prey to social engineering. In certain situations, employees examine patient records out of curiosity, breaking privacy rules. Such occurrences are frequently the result of inadequate access control measures or a lack of regular auditing and monitoring. Overall, these risks demonstrate that EHR cybersecurity is a sociotechnical challenge in which people, processes, and technologies interact to increase or degrade protection (Triplett, 2024)

Data Breaches and Unauthorized Access

Healthcare firms are attractive candidates for data breaches because of the high value of medical data. Unlike credit card information, which can be replaced, personal health information (PHI) contains immutable data such as medical history, genetic information, and insurance identifiers, which can be used for years.

Data breaches in healthcare have increased drastically over the last decade, both in frequency and in size. One of the most significant breaches occurred in 2015, when Anthem Inc., a major US health insurance company, experienced unauthorized access to its database. The hack affected roughly 78.8 million people. Hackers obtained names, social security numbers, medical IDs, and job information, exposing major flaws in identity management and network monitoring (Jiang *et al.*, 2025; Looi *et al.*, 2024).

Unauthorized access also occurs within organizations. Nurses and administrative personnel have occasionally viewed the records of celebrities or acquaintances without medical grounds, a flagrant violation of confidentiality. Such misuse highlights the necessity of role-based access control (RBAC) systems, which limit access based on job function, as well as audit trails that record every data access event. The consequences of data breaches go beyond financial penalties. They weaken patients' trust and discourage people from completely providing sensitive information to

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

healthcare providers (Tiwo et al, 2025). According to Looi et al. (2024), breaches can cause psychological harm to patients, particularly those in psychiatric care who may fear stigma or prejudice if their data are disclosed. Thus, data breaches are not only a technical and legal concern, but also an ethical one.

Interoperability Challenges

One of the primary goals of EHR systems is interoperability, which refers to the easy interchange of information between various healthcare institutions, laboratories, pharmacies, and insurers. Interoperability improves coordination and continuity of care, but it also increases the attack surface of healthcare systems (Tsai *et al.*, 2020). When EHRs communicate data across multiple platforms, each connection is a potential entry point for malicious actors. Poorly secured APIs, uneven encryption standards, and insufficient authentication can all lead to illegal access during transmission (Tsai *et al.*, 2020). According to Keshta and Odeh (2021), without uniform encryption standards, data sent between hospitals and external systems can be intercepted or manipulated. Furthermore, when many entities manage the same patient data, liability for security breaches can become muddled. According to Keshta and Odeh (2021), without uniform encryption standards, data sent between hospitals and external systems can be intercepted or manipulated. Furthermore, when many entities manage the same patient data, liability for security breaches can become muddled.

A major challenge is striking a balance between data availability and privacy. In emergency treatment, medical professionals must quickly access a patient's records across multiple systems, yet this can contradict rigorous privacy policies. Inconsistent consent handling further complicates interoperability. Patients may consent to data sharing inside one network but not another, but poorly built systems may fail to implement their preferences consistently. These interoperability issues show that technical integration without strong control might jeopardize both patient safety and confidence. Secure data interchange necessitates not only compatible software but also consistent legal, ethical, and policy frameworks (Schwappach et al, 2024).

Cloud Storage and Third-Party Vendors

Cloud computing has transformed healthcare data management, enabling scalable storage, faster access, and lower expenses. However, transferring EHR systems to the cloud creates new vulnerabilities that must be carefully addressed. When healthcare organizations outsource data storage or analytics to third-party providers, they essentially expand their trust boundaries beyond their own capabilities. According to Keshta and Odeh (2021), even respected manufacturers can be vulnerable to misconfigured cloud servers, insufficient encryption, or weak user authentication processes, resulting in significant data exposure. Another danger arises from unclear contractual obligations between providers and vendors. In shared environments, it is often unclear who is responsible for data security, whether the healthcare organization or the cloud provider. This shared responsibility gap might cause delays in responding to breaches and leave some risks untreated. Third-party analytics businesses, mobile application developers, and insurance partners frequently access subsets of EHR data for legal purposes such as research or billing. However, these external businesses may not necessarily adhere to healthcare-level security norms, posing additional risk. Ewoh and Vartiainen (2024) emphasize that a chain is just as strong as its weakest link: if one manufacturer fails to patch a vulnerability or monitor network activity, the entire EHR ecosystem is susceptible. To reduce these risks, robust data governance mechanisms are required. These include regular vendor audits, data encryption in transit and at rest, multi-factor authentication, and stringent Service Level Agreements (SLAs) that specify security expectations and consequences for noncompliance.

ADVANCES IN EHR DATA SECURITY

As healthcare becomes more digital, preserving Electronic Health Records (EHRs) has evolved from a compliance concern to a key technological and ethical issue. Traditional defense systems, such as passwords and firewalls, are unable to combat new cyberattacks. As a result, researchers and developers are currently concentrating on next-generation systems that use cryptography, blockchain, artificial intelligence (AI), and enhanced authentication techniques to protect EHR data. These improvements seek to improve secrecy, integrity, and availability. This section looks at five important breakthroughs that are influencing the future of EHR data protection.

Encryption and Access Control

Encryption remains very significant to healthcare cybersecurity. It encodes sensitive data in unreadable formats, which can only be decrypted

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

by authorized users. Conventional encryption algorithms, such as the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA), are still commonly employed in EHR systems because of their good balance of efficiency and strength. For example, most hospitals use AES-256 encryption to protect data housed in cloud environments. Meanwhile, RSA and elliptic curve cryptography (ECC) are widely used for secure data transmission between devices (Zhang *et al.,* 2022). Beyond regular encryption, homomorphic encryption and attribute-based encryption (ABE) are proving to be effective tools in healthcare. Homomorphic encryption enables computations on encrypted data without first decrypting it, allowing researchers to study patient data while protecting privacy. ABE, on the other hand, allows for fine-grained access control, with access permissions based on user criteria such as role or department rather than simple user IDs (Zhang *et al.,* 2022).

Access control enhances encryption by limiting who can see, edit, or distribute certain data. Modern EHRs use Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) to prevent insider misuse. These systems assign rights based on users' therapeutic roles; thus, a pharmacist cannot view psychotherapy notes, and a nurse cannot alter billing data. Simply put, encryption prevents outsiders from reading patient data, and access control guarantees that insiders only view what they are supposed to (Akinade, S.K., 2024).

Blockchain Applications

Blockchain technology's distributed and tamper-proof nature creates a new approach for securing health data. It is practically hard to change or remove records in EHRs without being noticed, since blockchain may act as a secure audit trail that documents every transaction, including who viewed or changed the data (Sharmin *et al.,* 2025).

Each "block" in a blockchain includes a cryptographic hash of the previous block, which ensures immutability. This characteristic enables healthcare facilities to automatically validate data integrity. Furthermore, blockchain-based EHR systems can provide decentralized consent management, allowing patients to govern data-sharing permissions using smart contracts. This encourages transparency and gives people the ability to choose who can access their records and for what purpose (Tariq *et al.,* 2025).

For example, a blockchain-enabled EHR may record that Dr. Smith accessed patient A's test results at 9:00 a.m. on a specific day. If someone tries to tamper with that record, the mismatch in the cryptographic chain will quickly reveal the change. Despite its potential, blockchain has scaling issues, such as high computing costs and latency. To overcome these hurdles, hybrid solutions that include blockchain and cloud infrastructure are being developed (Sharmin *et al.,* 2025).

AI and Machine Learning for Threat Detection

AI and machine learning (ML) are transforming cybersecurity by allowing predictive and adaptive defenses. Instead of relying exclusively on static firewalls or predetermined rules, AI-powered systems continuously learn from network activity and detect anomalies that could indicate a breach (Ali *et al.,* 2025). In EHR systems, machine learning algorithms monitor access logs, user behavior, and system events to detect strange activity patterns, such as when a nurse suddenly views hundreds of records outside of their unit or at odd hours. Real-time analysis enables early detection of insider threats and credential theft. At a large integrated delivery network in the United States led by the University of California, San Diego, researchers used machine learning (logistic regression and SVM) to audit and assess EHR access records. The SVM model outperformed baseline rule-based techniques on independently investigated suspicious occurrences, with an AUC of 0.95 and a sensitivity of 0.79 (Boxwala *et al.,* 2011). Another U.S. hospital-network study (Niu *et al.,* 2025) used various ML models and graph algorithms across a network of hospitals to find anomalies in EHR data routes and user-access patterns, detecting system-wide dangers rather than single-site events.

Deep learning models can even detect zero-day attacks, which use vulnerabilities unknown to system creators. AI also improves incident response by automating threat containment processes like locking compromised accounts and isolating infected devices. In the long run, combining AI-based monitoring with encryption and access control results in an adaptable security framework that adapts to meet emerging threats (Akinade S.K., 2024).

Multi-Factor Authentication and Biometric Security

One of the simplest and most effective ways to improve EHR security is to tighten user

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

authentication. Traditional single-password systems are particularly sensitive to phishing and credential theft. Multi-factor authentication (MFA) mitigates this by forcing users to validate their identity using at least two methods: something they know (password), something they have (smart card or token), and something they are (biometric trait) (Ficek *et al.*, 2021).

Biometric authentication, which includes fingerprint scanning, facial recognition, and iris scanning, provides an extra layer of identity protection that is difficult to forge or steal. In hospitals, medical professionals can now employ fingerprint-based logins to gain faster access to patient charts while ensuring security. According to research, adopting multi-factor authentication (MFA) and biometric systems reduces occurrences of unwanted access dramatically (Suleski *et al.*, 2023). For example, after implementing biometric access in one US hospital network, unauthorized login attempts decreased by more than 40%. When paired with behavioral analytics, such as identifying when a user signs in from an odd device or location, MFA systems can dynamically adjust their verification level, balancing usability and security (Triplett, 2024).

Secure Interoperability Standards

Secure interoperability standards, such as Health Level Seven (HL7) and Fast Healthcare Interoperability Resources (FHIR), are critical for ensuring safe data sharing between healthcare systems. These standards ensure that patient data shared throughout hospitals, laboratories, and insurance companies adheres to common formats and security regulations. HL7 standardizes the structure and terminology for exchanging clinical and administrative data. FHIR, developed by HL7 International, uses web technologies such as RESTful APIs and JSON to facilitate faster and more secure data transfer. FHIR also supports OAuth 2.0 and OpenID Connect, industry-standard protocols for secure authentication and authorization that ensure only certified entities have access to patient data (Salunkhe, V., 2024). For example, when a patient's EHR is shared between a hospital and an external specialist, FHIR ensures that data integrity is maintained and that the transfer takes place across encrypted, certified channels. These interoperability standards not only increase hospital efficiency, but they also promote security by requiring consistent, transparent data sharing methods.

Table 2. Summary of Cutting-Edge Technologies Used in EHR Security (Acar, *et al.*, 2018)

Technology	Main Function	Security Benefits	Limitation
AES, RSA, Homomorphic Encryption	Encrypt data at rest and in transit, enabling privacy-preserving computation	Prevents data leakages and supports secure research	High computational cost for large datasets
Blockchain	Distributed ledger for recording access and consent	Ensures immutability, traceability, and trust	Scalability and energy consumption issues
AI/ML Threat Detection	Monitors user behavior and system logs	Enables real-time anomaly detection and adaptive defense	Requires large datasets and continuous retraining
Multi-Factor Authentication and Biometrics	Verifies user identity using multiple credentials	Reduces credential theft and insider misuse	Costly hardware and user resistance
HL7/FHIR Standards	Defines secure data-sharing formats and APIs	Enhances interoperability and enforces encryption/authentication	Complexity of system integration

PRIVACY PRESERVATION IN ELECTRONIC HEALTH RECORDS (EHRS)

Maintaining privacy is the ethical and legal cornerstone of any Electronic Health Record (EHR) system. Because EHRs store highly sensitive and personally identifiable health information, privacy protection is not simply a technological concern, but also a legal and moral obligation. In the United States, two main federal laws, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, establish the criteria for protecting patient information (Osifowokan *et al.*, 2025). HIPAA's Privacy Rule grants patients control over their medical data,

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

including the opportunity to access, correct, and limit the disclosure of their information. The HITECH Act expanded these safeguards to electronic settings, requiring breach notifications and imposing harsher fines for noncompliance. Globally, regulations such as the European Union's General Data Protection Regulation (GDPR) emphasize consent, openness, and accountability when it comes to health data (Zhang *et al.*, 2022).

Modern EHR systems are increasingly employing privacy-preserving data approaches to ensure legal compliance. Anonymization permanently removes personal identifiers such as names and addresses from research datasets, making it impossible to re-identify individuals. Pseudonymization, on the other hand, replaces IDs with codes, allowing data to be connected back to patients when needed for follow-up care. Differential privacy, a privacy-preserving technique, introduces mathematical "noise" into data analysis, ensuring that aggregate results do not reveal information about any individual. These methods allow researchers and public health authorities to investigate population-level patterns without disclosing individual records (Ficek *et al.*, 2021).

Patient consent management is an equally crucial aspect of privacy. As healthcare becomes more digital and interconnected, it is becoming increasingly important to determine who owns medical data and who controls how it is utilized. Blockchain-based consent models are evolving, giving patients more control over their data. For example, a patient could authorize access to a specific therapist for a set time or revoke it immediately once therapy is completed. Such frameworks represent a patient-centered view of healthcare, restoring transparency and confidence (Tariq *et al.*, 2025).

KEY CHALLENGES IN PROTECTING EHRS

Despite major advancements, securing EHRs remains difficult on technical, organizational, and regulatory levels. One key difficulty is balancing security with usability. Healthcare personnel work in fast-paced situations where every second counts for patient outcomes. Overly rigorous security policies, such as frequent password resets or many login tiers, can cause delays and annoyance when accessing essential documents. These obstacles frequently encourage dangerous workarounds. The key difficulty is to create systems that preserve good security while not disturbing clinical workflows (Bani Issa *et al.*, 2020).

Another impediment is the high expense of integrating modern security technologies like AI-driven surveillance, blockchain infrastructure, and biometric authentication. Smaller clinics and rural hospitals frequently lack the financial or technical resources to implement these systems, exacerbating the security disparity between large and small facilities.

Regulatory and regulatory deficiencies impede protection efforts. Different governments interpret privacy rules differently, resulting in disparities in how patient data is treated cross-border. For example, HIPAA's US regulations diverge from GDPR's consent-based model, affecting international data transmission (Ewoh & Vartiainen, 2024).

Healthcare firms frequently struggle with legacy systems that were designed before modern cybersecurity requirements. Many hospitals continue to employ outdated operating systems or unpatched software that do not interact well with newer, more secure platforms. These antiquated infrastructures give easy access points for attackers. Another big problem is a lack of awareness and training among healthcare workers, which is still a huge human vulnerability. According to studies, many data breaches are caused by human error, such as clicking phishing links, using weak passwords, or leaving terminals unlocked. Regular security training, clear policies, and an accountable culture are critical to mitigating these threats (Triplett, 2024).

FUTURE CONSIDERATIONS FOR SECURING EHRS

The next generation of EHR security will most likely be differentiated by the incorporation of cutting-edge technologies, global collaboration, and a stronger emphasis on patient empowerment. Quantum-safe cryptography is growing as a research area to withstand the computational power of future quantum computers capable of breaking current encryption techniques. Similarly, zero-trust architectures, which assume that no person or device is inherently trustworthy, are being examined for healthcare networks. Every access request in this framework is continuously checked, lowering the risk of insider and lateral-movement assaults (Adeoye S. 2025).

Increased blockchain and AI use will improve data integrity and proactive threat detection. Future systems may incorporate blockchain to provide verifiable audit trails, while AI continuously

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

searches for irregularities across distributed networks. The combination of these methods could result in self-defending, intelligent EHR ecosystems that can learn from previous attacks. On the policy level, global harmonization of healthcare data-security standards is essential. As telemedicine and cross-border data sharing grow more common, global frameworks that align with HIPAA, GDPR, and other regional regulations will make compliance easier and increase privacy. Finally, patient-centric approaches in which individuals govern their data via digital wallets or consent dashboards reflect the ethical path for future healthcare. Giving patients the ability to choose when, how, and with whom their information is shared guarantees that privacy is a human right, not a technical afterthought (Lee, L. M., 2017).

CONCLUSION

Electronic Health Records (EHRs) have transformed healthcare by improving efficiency, coordination, and data accessibility. However, this digital shift has introduced challenges related to data security, privacy, and trust. While technologies like encryption, blockchain, AI, and biometric authentication have strengthened protection, issues such as legacy systems, high costs, and human error persist.

Future security efforts must focus on scalable, patient-centric frameworks. Innovations like quantum-safe cryptography and zero-trust architectures show promise, but success depends on global regulatory alignment and ethical data governance. Ultimately, securing EHRs is essential not just for preventing breaches but for preserving patient trust and ensuring safe, equitable healthcare delivery.

REFERENCES

1. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. “A survey on homomorphic encryption schemes: Theory and implementation.” *ACM Computing Surveys (CSUR)* 51.4 (2018): 1–35.
2. Adeoye, S. “Blockchain-enabled, post-quantum cryptographic framework for securing electronic health records: A next-generation approach to healthcare data protection.” 2025.
3. Akinade, S. K. “Implementing AI-driven anomaly detection for cyber-security in healthcare networks.” *ATBU Journal of Science, Technology and Education* 12.2 (2024): 598–610.
4. Ali, T. E., Ali, F. I., Eyvazov, F., & Zoltán, A. D. “Integrating AI models for enhanced real-time cybersecurity in healthcare: A multimodal approach to threat detection and response.” *Procedia Computer Science* 259 (2025): 108–119.
5. Anzalone, A. J., Geary, C. R., Dai, R., Watanabe-Galloway, S., McClay, J. C., & Campbell, J. R. “Lower electronic health record adoption and interoperability in rural versus urban physician participants: A cross-sectional analysis from the CMS quality payment program.” *BMC Health Services Research* 25.1 (2025): 128.
6. Bani Issa, W., Al Akour, I., Ibrahim, A., Almarzouqi, A., Abbas, S., Hisham, F., & Griffiths, J. "Privacy, confidentiality, security and patient safety concerns about electronic health records." *International nursing review* 67.2 (2020): 218-230.
7. Boxwala, A. A., Kim, J., Grillo, J. M., & Ohno-Machado, L. “Using statistical and machine learning to help institutions detect suspicious access to electronic health records.” *Journal of the American Medical Informatics Association* 18.4 (2011): 498–505.
8. Ewoh, P., & Vartiainen, T. “Vulnerability to cyberattacks and sociotechnical solutions for health care systems: Systematic review.” *Journal of Medical Internet Research* 26 (2024): e46904.
9. Ficek, J., et al. “Differential privacy in health research: A scoping review.” *Journal of the American Medical Informatics Association* 28.10 (2021): 2269–2276.
10. Häyrinen, K., Saranto, K., & Nykänen, P. “Definition, structure, content, use and impacts of electronic health records: A review of the research literature.” *International Journal of Medical Informatics* 77.5 (2008): 291–304.
11. Igwama, G. T., Olaboye, J. A., Maha, C. C., Ajegbile, M. D., & Abdul, S. "Integrating electronic health records systems across borders: Technical challenges and policy solutions." *International Medical Science Research Journal* 4.7 (2024): 788-796.
12. Jiang, J. X., Ross, J. S., & Bai, G. “Ransomware attacks and data breaches in US health care systems.” *JAMA Network Open* 8.5 (2025): e2510180.
13. Keshta, I., & Odeh, A. “Security and privacy of electronic health records: Concerns and challenges.” *Egyptian Informatics Journal* 22.2 (2021): 177–183.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

14. Lee, L. M. “Ethics and subsequent use of electronic health record data.” *Journal of Biomedical Informatics* 71 (2017): 143–146.
15. Looi, J. C., Looi, R. C., Maguire, P. A., Kisely, S., Bastiampillai, T., & Allison, S. "Psychiatric electronic health records in the era of data breaches–What are the ramifications for patients, psychiatrists and healthcare systems?." *Australasian Psychiatry* 32.2 (2024): 121-124.
16. McDermott, D. S., Kamerer, J. L., & Birk, A. T. “Electronic health records: A literature review of cyber threats and security measures.” *International Journal of Cyber Research and Education* 1.2 (2019): 42–49.
17. Mohammad, A. A. S., Alzyoud, M., Samara, E. I. M., Al-shanableh, N., Salameh, W. E. M. K. B., Alshurideh, M. T., ... & Al-Hawary, S. I. S. "Electronic health records adoption: a bibliometric analysis." *Intelligence-Driven Circular Economy: Regeneration Towards Sustainability and Social Responsibility–Volume 1*. Cham: Springer Nature Switzerland, 2025. 301-314.
18. Niu, H., Omitaomu, O. A., Langston, M. A., Grady, S. K., Olama, M., Ozmen, O., ... & Nebeker, J. "Anomaly Detection in Electronic Health Records Across Hospital Networks: Integrating Machine Learning With Graph Algorithms." *IEEE Journal of Biomedical and Health Informatics* (2025).
19. Osifowokan, A. S., Ahmed, Z., Adukpo, T. K., & Mensah, N. "Enhancing data compliance in the United States healthcare system: Addressing challenges in HIPAA and HITECH Act implementation." *EPRA International Journal. Https://doi. org/10.36713/epra21263* (2025).
20. Salunkhe, V. “Transforming healthcare research with interoperability: The role of FHIR and SMART on FHIR.” In *Healthcare Administration and Managerial Training in the 21st Century* (2024): 211–248. IGI Global.
21. Schwappach, D., Hautz, W., Krummrey, G., Pfeiffer, Y., & Ratwani, R. M. "EMR usability and patient safety: a national survey of physicians." *npj Digital Medicine* 8.1 (2025): 282.
22. Sharmin, S., Arefin, M. S., Dhar, P. K., Sultana, Z., & Akter, S. "A Scalable and Privacy-Preserving Hybrid Blockchain Architecture for Secure Healthcare Data Management." *International Journal of Advanced Computer Science & Applications* 16.8 (2025).
23. Shen, Y., Yu, J., Zhou, J., & Hu, G. "Twenty-five years of evolution and hurdles in electronic health records and interoperability in medical research: comprehensive review." *Journal of Medical Internet Research* 27 (2025): e59024.
24. Suleski, T., Ahmed, M., Yang, W., & Wang, E. “A review of multi-factor authentication in the Internet of Healthcare Things.” *Digital Health* 9 (2023): 20552076231177144.
25. Tariq, U. U., Sabrina, F., Rashid, M. M., Gordon, S., Lin, Y., Wang, Z., & Azad, S. "Blockchain-Based Secured Data Sharing in Healthcare: A Systematic Literature Review." *IEEE Access* (2025).
26. Tiwo, O. J., Adesokan-Imran, T. O., Babarinde, D. C., Salami, I. A., Onyenaucheya, O. S., & Olaniyi, O. O. "Improving patient data privacy and authentication protocols against AI-powered phishing attacks in telemedicine." *Asian Journal of Research in Computer Science* 18.4 (2025): 93-114.
27. Triplett, W. J. “Exploring and mitigating cybersecurity challenges in electronic health records.” *Cybersecurity and Innovative Technology Journal* 2.1 (2024): 41–52.
28. Tsai, C. H., Eghdam, A., Davoody, N., Wright, G., Flowerday, S., & Koch, S. "Effects of electronic health record implementation and barriers to adoption and use: a scoping review and qualitative analysis of the content." *Life* 10.12 (2020): 327.
29. Zhang, L., Xu, J., Vijayakumar, P., Sharma, P. K., & Ghosh, U. "Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare system." *IEEE transactions on network science and engineering* 10.5 (2022): 2864-2880.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Filani, A. and Opoku, J. A. " Protecting Electronic Health Records (EHRs): Advances and Challenges in Data Security and Privacy." *Sarcouncil Journal of Engineering and Computer Sciences* 4.12 (2025): pp 1-9.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher