



(RESEARCH ARTICLE)



ELECTRONIC HEALTH RECORD CYBERSECURITY: BALANCING INSIDER AND EXTERNAL THREAT PROTECTION WITH CLINICAL USABILITY AND PATIENT SAFETY

Adewumi Busayo Adelemi *

Division of Engineering and Computer Science, Oklahoma Christian University.

* Corresponding Author

International Journal of Science and Research Archive, 2026, 20(03), 803–805

Publication history: Received on 14 August 2026; revised on 20 September 2026; accepted on 22 September 2026

Article DOI: <https://doi.org/10.30574/ijrsra.2026.20.3.1810>

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

The healthcare sector has been revolutionized by the application of Electronic Health Records (EHRs) in digitizing healthcare, improving efficiency, and enhancing access to data within healthcare systems. Greater reliance on EHRs, however, has opened possibilities for exposure to insider and external threats. Insider threats are usually caused by the abuse of access rights by healthcare employees, while external threats are caused by cyberattacks such as ransomware, phishing, and data breaches. This paper explores the nature of insider and external threats to EHRs, evaluates existing security systems, and recommends methods such as access control, encryption, machine learning-based anomaly detection, and adherence to regulatory standards such as HIPAA. Through the integration of technology, organizational, and human aspects, healthcare systems can enhance EHR security while maintaining usability within clinical workflows.

Keywords: Electronic Health Records (Ehrs), Insider Threats, Cybersecurity, Data Breaches, Access Control, Machine Learning Anomaly Detection.

1 INTRODUCTION

Healthcare has undergone colossal transformation as patient data has been computerized, and Electronic Health Records (EHRs) implemented. EHRs provide unbridled access to patient information that enables more accurate diagnoses, more coordinated care, and improved outcomes (Menachemi & Collum, 2011). But this broader utilization of digital infrastructure has also multiplied the risk of data breaches, insider exploitation, and cyberattacks. Health care data breaches increased over 250% between 2010 and 2022, with millions of patient records compromised annually (HIPAA Journal, 2022).

EHR systems hold very intimate patient information, so they are a high-value target for cyberattacks. Unlike most other sectors, healthcare not only incurs financial consequences from violations but also clinical and ethical threats, including loss of patient trust and safety threatening (Raghupathi & Raghupathi, 2014). Insider attacks, where workers misuse their privileges, present a special threat because they often evade traditional security defenses. Outside breaches such as ransomware attacks may paralyze hospital operations, leading to delayed treatments and, in severe cases, death.

This paper explores insider and outside threats to EHRs, criticizes existing strategies to mitigate these threats, and proposes a framework that includes technology, policy-based, and people-centric interventions.

2 LITERATURE REVIEW

2.1 Insider Threats

Insider threats remain one of the most pervasive security problems for healthcare organizations. They occur when legitimate users intentionally or unintentionally violate EHRs. Studies show that healthcare providers often violate security policies in terms of negligence, curiosity, or malice (McLeod & Dolezel, 2018). For instance, "snooping" on the medical history of celebrities is one common category of insider misuse. Moreover, resentful employees have changed or stolen data for private use. Machine learning-driven anomaly detection has also been proposed as a strong solution to detect such activity (Alharthi et al., 2022).

2.2 External threats

External entities are another, yet equally dangerous, threat. Cybercriminals exploit relatively weaker cybersecurity systems in healthcare compared to other sectors such as finance. Ransomware attacks, for instance, the 2017 WannaCry attack, paralyzed world health systems, leading to delay in surgeries and diagnostic examinations (Martin et al., 2017). Phishing has remained a prevalent attack vector, with healthcare staff generally still under-educated in cybersecurity awareness. Black-market demand drives the extremely high value of health records, and they will probably be used for identity theft, insurance fraud, and misuse of prescription drugs (Ponemon Institute, 2021).

2.3 Regulatory and Policy Frameworks

Health Insurance Portability and Accountability Act (HIPAA) in the US demands safeguarding of protected health information (PHI). Compliance, however, even then, is not sufficient to guarantee total protection. Research identifies that more resilient organizations are those which shift beyond compliance to adopting continuous monitoring and active security cultures (Appari & Johnson, 2010).

3 METHODS/APPROACHES TO SECURITY

There must be a multi-layered strategy for protecting EHRs. The most critical methods are:

3.1 Access Control and Authentication

Role-based access controls (RBAC) restrict access to secured records based on job responsibilities. Multifactor authentication (MFA) adds an additional layer of protection against improper logins.

3.2 Encryption and Data Masking

Encryption of EHR data at rest and in transit ensures that even if intruders penetrate, the data is not accessible without decryption keys.

3.3 Machine Learning-Based Detection

Advanced algorithms can monitor user activity to look for abnormalities signaling insider misuse or external attacks (Alharthi et al., 2022).

3.4 Incident Response and Recovery

Implementation of rapid incident response processes minimizes downtime during cyberattacks. Backup systems and redundant storage are essential for recovering from ransomware attacks.

3.5 Training and Awareness

Human error is the leading cause of data breaches. Recurring staff training in phishing identification, password health, and compliance reinforces the security awareness culture (McLeod & Dolezel, 2018).

3.6 Regulatory Compliance and Auditing

Ongoing auditing and compliance with HIPAA, GDPR, and other directives are critical to maintaining data integrity and public trust.

4 DISCUSSION

The sophistication of healthcare environments dictates that no one measure is enough to protect EHRs. Encryption and access control are adequate starting points, but insider threats necessitate behavior monitoring and accountability. Machine learning-based systems offer promise in flagging suspicious access patterns, but they will have to walk the line between sensitivity to anomalies and reducing false positives that swamp IT staff.

Furthermore, healthcare organizations must realize that cybersecurity is as much an organizational and human problem as it is a technical one. Effective governance, appropriate security policies, and regular staff training are needed. Expenditure on cybersecurity must be balanced against clinical efficacy, or else systems become too restrictive to impede the ability of medical personnel to act in emergency care situations.

Finally, collaboration between public authorities, tech companies, and healthcare organizations is required. Threat actors' common sense, standardized security practices, and public-private collaboration can all increase resilience.

5 CONCLUSION

Balancing Insider and External Threat Protection with Clinical Usability and Patient Safety is an overarching challenge in today's healthcare. Insider misuse and external cyberattacks breach sensitive information, impair services, and threaten patient security. A holistic strategy that integrates technological safeguards, behavior monitoring, organizational culture, and regulatory mandates must be achieved. More studies must focus on advanced detection methods through artificial intelligence, as well as inter-state cooperation mechanisms in healthcare cybersecurity. With multi-level defense systems, health systems can safeguard patient trust and ensure continuity of care against constantly evolving cyber threats.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Acknowledgments

The author has no acknowledgements to declare

Disclosure of conflict of interest

To my knowledge, there are no conflicts of interest.

REFERENCES

- [1] Menachemi, N., & Collum, T. H. (2011). Benefits and drawbacks of electronic health record systems. *Risk Management and Healthcare Policy*, 4, 47–55.
- [2] HIPAA Journal. (2022). Healthcare data breach statistics. <https://www.hipaajournal.com/healthcare-data-breach-statistics/>
- [3] Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: Promise and potential. *Health Information Science and Systems*, 2(3), 1–10. <https://doi.org/10.1186/2047-2501-2-3>
- [4] McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, 108, 57–68.
- [5] Alharthi, R., Alhothali, A., & Alarifi, A. (2022). Securing electronic health records against insider threats: A supervised machine learning approach. *Healthcare Technology Letters*, 9(2), 55–63.
- [6] Martin, G., Ghafur, S., Cingolani, I., Symons, J., & Darzi, A. (2017). WannaCry—A year on. *BMJ*, 361, k2381.
- [7] Ponemon Institute. (2021). Cost of data breach report. IBM Security. <https://www.ibm.com/security/data-breach>
- [8] Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. *International Journal of Internet and Enterprise Management*, 6(4), 279–314.