IJHRIM

Intl J Health Recs & Info Mgt. Jan – Dec 2025;8(1):28-29

Research article

Print ISSN 2645-2464; E ISSN 2695-1770

Assessment of information security in electronic medical records management system at the University of Medical Sciences Teaching Hospital, Ondo, Nigeria

Oloruntoba Caleb Adebayo[1*],

[1]School of Health Information Management, University of IlorinTeaching Hospital, Ilorin, Nigeria

Corresponding author*: E-mail: *adebayooloruntoba21@gmail.com*

ABSTRACT

Background/Objectives: The adoption of electronic medical records (EMR) has transformed healthcare data management, but has raised concerns about information security. This study assessed the level of information security in the EMR system at the University of Medical Sciences Teaching Hospital (UNIMEDTH), Ondo. ***Design/Methods:*** A descriptive survey design was employed, with data collected from 124 Health Information Management (HIM) professionals and 10 patients. ***Results*** Results revealed strong awareness of EMR and high confidence in data security among staff and patients, but challenges such as inadequate funding, poor record management policies and limited storage facilities persist. ***Conclusion:*** The study concludes that while awareness and usage of EMR are high, systemic issues must be addressed to ensure sustainable data security. Recommendations include improved policy implementation, staff training and investment in infrastructure.

Keywords: *Data protection; Electronic medical records; Information security; Health information management; Nigeria*

Edited by *QB Suleiman-Abdul; submitted on 12.06.2025 peer reviewed by M Achinbee, U Isah; accepted 24.06.2025; published 29.06.2025.*

Please cite as: *Adebayo OC. Assessment of information security in electronic medical records management system at University of Medical Sciences Teaching Hospital, Ondo. Int J Health Recs & Info Mgt. 2025;8(1):28-29.*

Conflict of interest: None declared.

Funding disclosure: No funding was solicited for nor obtained for this study

INTRODUCTION

Nigeria's medical records management has evolved from undocumented traditional practices to the modern digital systems seen today. Early records were maintained manually with formal records management gaining ground post-1960s[1]. The establishment of the Nigerian Association of Medical Records Officers in 1966 marked a turning point in the professionalization of the field. Electronic medical records (EMR) also referred to as computerized health records, have become a central component of modern healthcare[1]. These systems enable the systematic collection and exchange of patient data across health systems, enhancing the quality and continuity of care[2]. Increased digitalization has however laid significant concerns regarding the confidentiality, integrity and availability of health data[3]. The computerization of health records has brought substantial improvements in data accessibility and care coordination. Electronic medical record systems consolidate patient information from various departments, facilitating real-time updates, structured documentation and machine-assisted decision-making [4].

Healthcare systems in developing countries such as Nigeria often face challenges in implementing secure EMR systems. Barriers include technological inadequacies, limited funding, resistance from healthcare professionals and unauthorized data access and cyber threats [5-7]. Information security technologies such as firewalls, encryption, biometrics and user authentication are essential to maintaining confidentiality, integrity and availability of health data[8,9]. Addressing these issues is critical to building effective and secure health information systems. Laws such as the Health Insurance Portability and Accountability Act (HIPAA) in the US and the Health Records and Information Privacy Act (NSW, Australia) emphasize patient consent and data protection[10]. Consent mechanisms, if poorly implemented, may hinder clinical workflows or compromise patient care[11].

This study aim to assess information security in the EMR management system at UNIMEDTH, Ondo, by understanding the concept of information security within EMR systems, identifying the existing security technologies used, investigating the challenges in managing EMR in public hospitals and evaluating the importance of information security in EMRs.

METHODS

A descriptive research design was employed. The population consisted of 124 HIM professionals and 10 randomly selected patients at UNIMEDTH. Purposive sampling was used. Data collection involved self-administered questionnaires with both closed-ended questions and structured interviews. Descriptive statistics, including frequency counts and percentages, were used for analysis.

RESULTS

1. **Awareness:** 100% of HIM staff were aware of EMR; 95.8% were aware of information security.
2. **Security Practices:** Most participants (95.8%) reported that username and password were the primary security measures; however, biometrics were viewed as more secure.
3. **Challenges:** Inadequate funding (100%), insufficient trained personnel (100%) and lack of policies (69.7%) were reported as major challenges.
4. **Perceived Importance:** All participants agreed that information security supports accurate records, patient care, legal processes, and research.

DISCUSSION

Despite high awareness and usage, the reliance on basic security measures like user names and passwords indicates a gap in adopting more advanced technologies such as biometrics and encryption[2]. Challenges such as funding constraints and lack of policy infrastructure hinder effective implementation[6]. Furthermore, staff training and compliance with data protection laws remain crucial for sustainable information security[5].

CONCLUSION

Electronic medical records significantly enhance healthcare delivery by improving data accessibility, coordination and accuracy. Robust information security measures must be implemented to protect patient data. The findings underscore the need for a comprehensive approach to policy, infrastructure and training to ensure data protection in healthcare settings.

Recommendations

1. Implement standardized record management policies and security protocols.
2. Upgrade security mechanisms beyond username-password authentication.
3. Allocate sufficient funding for information security infrastructure.
4. Train HIM professionals in data privacy and EHR best practices.
5. Advocate for national legislation on health information protection.

REFERENCES

1. Iwhiwhu BE. *Records management at NEPA headquarters, Lagos, Nigeria* (Unpublished master's thesis). University of Ibadan, 1998.
2. Millar L. The right to information: The right to records. *Commonwealth Human Rights Initiative*, 2003. http://www.humanrightsinitiative.org/programs/ai/rti/articles/record_keeping_ai.pdf
3. Hufford M. Patient data confidentiality and electronic health records. *Health Management Quarterly*. 1999;3(1):12–18.
4. Amatayakul M. *Electronic health records: A practical guide for professionals and organizations*. AHIMA Press, 2004.
5. Alexis J. *Information management in healthcare systems*. Springer, 2012.
6. Roper M, Millar L. *Managing hospital records*. International Records Management Trust, 1999. https://www.irmt.org/documents/educ_training/public_sector_rec/IRMT_hospital_recs.pdf
7. Gaithersburg M. *Cybersecurity in health care systems*. National Institute of Standards and Technology, 2000.
8. Anderson R. *Security engineering: A guide to building dependable distributed systems*. Wiley, 1999.
9. Chilton SM, Bates DW, Leape LL. Privacy and security in electronic health records. *Journal of Health Informatics*. 1999;4(2):35–47.
10. Coiera E, Clarke R. E-consent: The design and implementation of consumer consent mechanisms in an electronic environment. *Journal of the American Medical Informatics Association*. 2004;11(2):129–140. doi:10.1197/jamia.M1359.
11. Win K, Croll P, Cooper D. Electronic health records and patient consent. *Electronic Journal of Health Informatics*. 2003;1(1):21–30.

AOC conceived of the study, initiated the design, participated in literature search and data collection, analysis and coordination. He wrote and reviewed the final manuscript.