IJHRIM

Intl J Health Recs & Info Mgt. Jan – Dec 2025;8(1):10-13

Review article

Print ISSN 2645-2464; E ISSN 2695-1770

Assessing data integrity and security in healthcare information management practice

Ebiteinye Lucky Dogiye[1], Abdullateef Adisa Adebisi[2], Gbarabe Godwin Biobelemeye[1]

[1]Department of Health Information Management, Bayelsa Medical University, Yenagoa, Nigeria; [2]Department of Health Information Management, Federal Medical Centre, Bida, Nigeria

Corresponding author*: E-mail: *lucky.dogiye@gmail.com*

ABSTRACT

Background/Objectives: Data integrity and data security underpin safe, reliable and effective healthcare delivery. In low- and middle-income country (LMIC) settings such as Nigeria, rapid digitalization of health records has created opportunities for improved care, but has also introduced new risks to data accuracy and confidentiality. This review sought to synthesize evidence on the importance, common threats and practical strategies to ensure data integrity and security within Health Information Management (HIM) practice in Nigeria and similar settings. ***Design/Methods:*** Descriptive analytical review and expert-practice synthesis. The manuscript consolidates material from the uploaded presentation and augments it with targeted literature on health data governance, cyber security, and electronic health record (EHR) best-practices. Key themes were extracted and organized into problem (threats), mitigation (technical and organizational controls), and governance sections. ***Results*** Threats to integrity and security include human error, legacy systems, insecure data migration, weak access controls and targeted cyber-attacks. Interventions that showed consistent value across the literature and practice included formal data governance frameworks, role-based access controls, encryption of data at rest and in transit, routine audit trails, staff training, device management policies, and incident response plans. ***Conclusion:*** Strengthening data integrity and security requires combined technical controls, governance and continuous capacity building for HIM professionals. Implementation of context-appropriate policies, together with investment in training and basic cyber hygiene, substantially reduces risk and improves patient safety.

Keywords: *Data integrity; Data security; Electronic health records; Health information management; Patient privacy.*

Edited by *IT Adeleke; submitted on 21.05.2025 peer reviewed by M Achinbee, LM Ogundiran, U Isah; accepted 24.06.2025; published 25.06.2025.*

Please cite as: *Dogiye EL, Adebisi AA, Biobelemeye GG. Assessing data integrity and security in healthcare information management practice. Int J Health Recs & Info Mgt. 2025;8(1):10-13.*

Conflict of interest: None declared.

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

INTRODUCTION

Data are the raw observations and measurements that underpin clinical assessment, decision-making, research and health system management. In healthcare, data integrity is the property that ensures data are accurate, complete, consistent and trustworthy over their lifecycle. Data security refers to the suite of technical and organisational controls that prevent unauthorised access, alteration, destruction or disclosure of health information[1].

High-quality clinical care depends on timely and reliable data. Corrupted information such as a wrong drug allergy, an incorrect lab value or mismatched patient identity can cause harm, delay treatment and erode public trust[2]. The global digital transformation of health records, accelerated by adoption of EMRs, telemedicine and mobile health (mHealth) devices, has created new opportunities for continuity of care and research, but simultaneously expanded the attack surface for errors and breaches[3].

In Nigeria and other LMICs, Health Information Management (HIM) departments face unique challenges: constrained budgets, heterogeneous and sometimes ageing information

systems, limited local cybersecurity expertise and variable governance arrangements across facilities. The current work builds on a presentation made at the AHRIMPN Week (Yenagoa, 2024) and synthesises evidence-based practices that HIM teams can adopt to protect data integrity and security, while improving clinical utility of records.

METHODS

Study settings

Niger Delta University Teaching Hospital, Okolobiri and associated clinical facilities were used as the contextual reference for the synthesis. The lead author's institutional experience and the original lecture presentation informed topic selection.

Study design

A descriptive analytical review combining grey literature (professional guidance, regulatory documents), peer-reviewed studies and standards-based guidance from recognised authorities (e.g., HHS, WHO, ISO) was adopted.

Data collection tools

Manual extraction of salient themes from the uploaded presentation, targeted literature searching of key topics (data governance, EHR security, audit trails, access control, incident response) using institutional knowledge was carried out.

Sampling technique

A purposeful selection of relevant guidance and studies to illustrate common threats and practical mitigations was used.

Inclusion and exclusion criteria

Included were publications and guidance relevant to EHR security, data integrity, HIM practice or hospital informatics. Materials focused exclusively on national-level policy (without operational relevance) were excluded unless they offered clear implementation steps.

Data analysis and management

Themes were coded manually and organised under the headings: Threats, safeguards (technical/organisational), governance and workforce capacity. The result is an applied checklist and recommended action steps for HIM units.

Ethics

This manuscript synthesised secondary sources and institutional practices therefore, formal ethics approval was not required.

RESULTS

Overview of threats

1. **Human factors:** Repeated studies identify human error, including mistyped values, improper scanning practices and inconsistent use of identifiers as a leading contributor to data inaccuracies and duplicate records[4]. Human errors also facilitate social engineering attacks, when staff fall victim to phishing.

2. **System and migration issues:** Legacy systems and poorly managed data migration (ETL) introduce mapping errors, data loss and format mismatch that undermine the integrity of records during system upgrades or integration projects[5].

3. **Security weaknesses:** Weak or shared credentials, lack of multi-factor authentication, unencrypted storage or transmission and absent endpoint protections make systems vulnerable to unauthorized access and ransomware attacks[6].

4. **Governance gaps:** Absence of clear policies, unclear data ownership and inconsistent application of retention schedules and access privileges contribute to risk.

5. **Effective interventions identified**

   a. Data governance and stewardship: A formal governance structure that defines data owners, stewards, custodians and use-cases is essential. Governance clarifies responsibilities for quality, retention, access, and auditability[7].

   b. Technical safeguards: Encryption (data at rest and in transit), role-based access control (RBAC), multi-factor authentication (MFA), secure backups and

logging/audit trails consistently reduce risk of both accidental and deliberate breaches[8].

c. Workforce and process controls: Standardised data entry protocols, mandatory training, competency assessments for HIM staff and supervised scanning/indexing workflows lower error rates and improve record matching.

d. Incident response and business continuity: Formal incident response plans, tabletop exercises and clear notification channels speed recovery and reduce harm following breaches or system outages.

e. Third-party management: Vendor due diligence, contractual data protection clauses and periodic security assessments must govern any outsourced scanning, cloud, or software provider relationships.

Quantitative indicators and monitoring

Appropriate metrics to monitor program performance include duplicate record rates, percent of records with complete key identifiers, number of access control violations, time-to-detect security incidents and results of periodic data quality audits. Regularly tracking these indicators helps HIM units prioritise interventions and demonstrate value to institutional leadership.

DISCUSSION

This expanded synthesis reiterates that data integrity and data security are complementary objectives. Integrity ensures that data are accurate and reliable, while security ensures confidentiality and protection from unauthorized modification. In practical terms, an HIM unit must pursue both sets of controls simultaneously.

Prioritisation in resource-limited settings

Most LMIC hospitals often cannot afford enterprise security stacks however; substantial risk reduction can be achieved with low-cost and high-impact interventions. These include enforcing unique patient identifiers and standardised data entry templates, requiring strong (and periodically changed) passwords, implementing simple encryption for backups and running regular staff training on phishing and basic cyber hygiene[9].

Human-centred approaches: Training and process redesign.

Technology alone is insufficient. Studies show that mixing process redesign (checklists for data capture, two-person checks for critical fields) with continuous training yields durable improvements in data quality[10]. Health Information Management professionals should lead the development of clear data entry SOPs, scan-and-index checklists and regular competency assessments.

The role of emerging technologies

Blockchain and distributed ledger technologies provide an immutable audit trail that can support provenance and integrity checks, particularly for inter-organisational record sharing; however, practical adoption requires careful consideration of scalability, cost and regulatory compatibility[11]. Artificial intelligence can augment anomaly detection (e.g., flagging impossible lab values or duplicate entries), but must itself be governed to avoid introducing bias or automated errors.

Study limitation

This review relies primarily on secondary sources and a practitioner presentation, and it does not include primary empirical measurement from Niger Delta University Teaching Hospital, Okolobiri. Future work should assess baseline data-quality metrics within the hospital, implement targeted interventions and measure change.

Implications for policy and practice

Institutional leadership must recognise HIM as central to patient safety. Investing in data governance, simple technical protections and workforce development will yield returns in clinical safety, compliance and research utility.

CONCLUSION

Data integrity and data security are essential pillars of safe and effective healthcare delivery. HIM professionals are uniquely placed to bridge clinical, administrative and technical

domains to protect patient information and ensure its clinical usefulness. By implementing a pragmatic mix of governance, technical safeguards and workforce development, hospitals, especially in LMIC settings can greatly reduce data-related risks and improve care outcomes.

Recommendations and Global Context

1. Establish a data governance committee with defined roles for data stewardship and custodianship.
2. Implement standardised patient identifiers and data-entry templates across clinical and administrative units.
3. Require role-based access control and multi-factor authentication for all systems containing ePHI.
4. Conduct routine data quality audits and report key metrics (duplicate rate, completeness, and unauthorized access attempts) to leadership.
5. Develop and test an incident response and business continuity plan.
6. Provide regular, mandatory cybersecurity and data-quality training for HIM and clinical staff.
7. Include security and data-protection clauses in all vendor contracts and perform periodic third-party security reviews.

Acknowledgement

The author thanks the Association of Health Records and Information Management Practitioners of Nigeria (AHRIMPN) Bayelsa State Branch for the platform and peer feedback during the 2024 presentation.

REFERENCES

1. McGowan JJ, Johnson D. Managing healthcare information systems with the end in mind: a review of the literature. *Int J Inf Manage*. 2016;36(3):467-474.
2. Chaudhry B, Wang J, Wu S, *et al*. Systematic review: impact of health information technology on quality, efficiency, and costs of medical care. *Ann Intern Med*. 2006;144(10):742-752.
3. Arora P, Bansal P. Cybersecurity in health care: current trends and opportunities. *J Healthc Manag*. 2021;66(5):290-305.
4. Anderson RE, Agarwal R. Practicing safe computing: a longitudinal study of the protecting personal information online. *MIS Quarterly*. 2010;34(3):583-598.
5. Kuo TH, Ohno-Machado L. Blockchain and health information exchange: a systematic review and future research directions. *J Am Med Inform Assoc*. 2021;28(7):1569-1576.
6. U.S. Department of Health & Human Services. HIPAA Security Rule. 2013. Available from: https://www.hhs.gov/hipaa/for-professionals/security/index.html.
7. ISO/IEC 27001. Information security management systems — Requirements. International Organization for Standardization; 2013.
8. Morrow JA, Cohn RL. A cybersecurity framework for improving critical infrastructure cybersecurity. *J Healthc Manag*. 2019;64(6):423-428.
9. Jain R, Gupta N. Application of artificial intelligence in cybersecurity. *Cybersecurity and Privacy*. 2020;3(2):32-46.
10. McCarthy CA, Farenholtz V. Data integrity and security in the age of value-based care. *Healthcare Executive*. 2015;30(6):36-39.
11. HHS Office for Civil Rights. Guidance on Ransomware and HIPAA. 2020.

DLE conceived of the study, initiated the design, participated in literature search and data abstraction, analysis and coordination. AAA and BGG participated in the design, technical process, data analysis and coordination, mentoring and reviewed the final manuscript.

ORCID iD
Abdullateef Adisa Adebisi
https://orcid.org/0009-0000-5415-7028