Nigerian Medical Journal
NIGERIA MEDICAL ASSOCIATION
Print ISSN 0300-1652, E-ISSN 2229-774X

Expert Opinion

The Role of Cybersecurity Education in Nigeria's Healthcare Sector

Christian Idenobe Odion[1], Emmanuel O. Oisakede[2,3]

[1]Department of Cybersecurity, Wellspring University, Edo State, Nigeria. [2]Department of Clinical Oncology, Leeds Teaching Hospitals NHS Trust, Leeds, United Kingdom. [3]Department of Health Research, University of Leeds, Leeds, United Kingdom.

Abstract

Nigeria's uptake of digital health through electronic records, telemedicine and connected devices has expanded the cyber-attack surface of health facilities. Cybersecurity failures are not only data-governance problems; they can interrupt prescribing, diagnostics, referral pathways and emergency workflows, with downstream implications for patient safety and trust. Evidence from hospital incidents shows that ransomware and recovery efforts can disrupt services and degrade the timeliness of care when staff are unprepared, underscoring the need to treat cyber resilience as a clinical quality domain.

This letter argues that the most scalable risk reduction in low-resource settings is workforce capability: many healthcare breaches exploit human and workflow weaknesses rather than novel technical exploits. We outline a minimum, role-based cybersecurity education package for medical students and practicing clinicians covering: (1) governance, policies and third-party risk management; (2) core technical controls clinicians encounter daily (access control, encryption, patching, segmentation and logging); (3) training and awareness focused on phishing, social engineering and safe downtime workarounds; (4) incident response and recovery integrated into clinical continuity planning; and (5) compliance and ethics aligned to Nigeria's data protection requirements.

Embedding these competencies in curricula, accreditation and continuing professional development, reinforced through drills and monitoring, can protect sensitive information and keep essential services running during disruption.

***Correspondence:** Emmanuel O Emmanuel.oisakede@gmail.com, ORCID: https://orcid.org/0009-0000-5791-301X

How to Cite: Odion CI, Oisakede EO. The Role of Cybersecurity Education in Nigeria's Healthcare Sector. Niger Med J 2026; 67 (2):3235-3239. http:// doi.org/10.71480/nmj.v67i2.969

Quick Response Code:

To the Editor,

Digital health is becoming routine across Nigeria, from the Nigeria Digital in Health Initiative (NDHI) and expanding electronic medical records to telemedicine and mobile health applications [1]. The World Health Organization (WHO) has emphasised that digital health should be implemented in ways that are ethical, safe, secure, and privacy-preserving [2]. However, with increasing cyberattacks on digital platforms used by health facilities, cybersecurity is not a peripheral technical concern; it is a patient-safety requirement and a prerequisite for trustworthy, sustainable care delivery.

Healthcare is a particularly attractive target for attackers because clinical data are highly sensitive and difficult to remediate once exposed, while service disruption can immediately affect diagnosis, prescribing, referrals, and emergency workflows [3-6]. Evidence shows that cyber incidents can translate into measurable operational and clinical harm. A multicentre study of US emergency departments found that ransomware events were associated with disruptions at neighbouring facilities [7]. A separate hospital case study documented how a ransomware attack disrupted surgical training and hospital operations [8]. Importantly, post-breach remediation efforts have also been associated with deterioration in timeliness of care and acute myocardial infarction outcomes, highlighting that poorly integrated security responses can unintentionally degrade care if staff are not prepared [9].

Systematic reviews describe a broad threat landscape in healthcare, including ransomware, phishing, malware, and vulnerabilities arising from complex sociotechnical systems [3–6]. Phishing and social engineering remain frequent initial access vectors [10,11]; malware and delayed patching enable persistence in environments dominated by legacy devices and uptime-sensitive systems [3,6]; insider threats (malicious or inadvertent) expose records and weaken accountability [3,6]; and supply chain attacks exploit third-party vendors, shared platforms, and outsourced services [12]. The rapid growth of Internet of Medical Things (IoMT) devices adds further risk when procurement, configuration, and maintenance do not embed security requirements [13].

Education is central because many attacks succeed through human and workflow weaknesses rather than technical failure alone. Reviews of human factors in healthcare cybersecurity consistently point to gaps in awareness, security culture, and role clarity as recurrent contributors to incidents [6,14]. Yet cybersecurity competencies are still inconsistently embedded across health professional training, and workplace learning frequently prioritises "how to use" digital tools over "how to use them safely" [15]. This gap is especially consequential in low-resource settings where shared workstations, intermittent connectivity, limited backups, and constrained IT staffing can amplify the impact of otherwise preventable errors.

To close this gap, cybersecurity education needs to be framed as a clinical competency, delivered across the training pipeline (undergraduate, internship/residency, and continuing professional development) and tailored to clinical roles. A minimum, role-based package for medical students and healthcare practitioners is outlined below.

1. Strategies and policies (governance and risk management)

Training institutions and health facilities should teach practical governance: data stewardship, risk assessment, asset inventory, safe configuration, and vendor/third-party risk management. Organisational approaches emphasise that technical controls are most effective when coupled with clear policy, leadership accountability, and an enabling safety culture [6,16]. Nigeria-specific modules can map clinical processes (registration, prescribing, laboratory, imaging, referral, billing) to risks and controls, and align local policies to recognised frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [17] and security-by-design approaches used in cyber range training and simulation [18].

2. Technology controls (basic protections for systems and data)

Curricula should expand and explain the controls clinicians encounter daily: multifactor authentication, role-based access, encryption for data at rest and in transit, secure mobile-device use, patching, network

segmentation, endpoint protection, and logging. Teaching should link controls to bedside consequences (e.g., how credential sharing undermines audit trails; how delayed patching increases exposure of imaging and laboratory systems). The NIST catalogue of security and privacy controls provides a practical reference for building locally appropriate baselines, including specific families for access control, audit, configuration management, contingency planning, and incident response [19].

3. Training and awareness (human factors)

Regular, role-specific training should cover phishing recognition, safe handling of links and attachments, password hygiene, social engineering prevention, and secure workarounds during downtime. Evidence-based approaches in healthcare include recurring simulations with feedback and targeted reinforcement for higher-risk job roles [10,11]. Behavioural research among healthcare professionals shows that perceived severity and response efficacy meaningfully influence security intentions, supporting the use of training that makes clinical consequences explicit and demonstrates practical coping actions [20].

4. Incident response and recovery (clinical continuity)

Every facility should teach a simple incident response playbook, i.e., how to recognise warning signs, report quickly, isolate affected devices, preserve evidence, and maintain essential services using planned downtime procedures. Table-top exercises and drills can be integrated into quality-improvement activities and clinical simulation, ensuring staff can safely transition to analogue workflows when systems are unavailable [21]. Lessons from ransomware recovery in imaging operations emphasise the need for phased recovery planning, incident communication structures, and ongoing readiness exercises [22].

5. Compliance and ethics (legal and professional duties)

Cybersecurity education should reinforce confidentiality, informed consent for data sharing, and the ethical handling of sensitive records. Compliance modules should cover Nigeria's data protection requirements and workforce training expectations, alongside practical documentation and reporting duties, consistent with global calls for secure, privacy-preserving digital health [2,23,24]. Linking legal obligations to professional ethics helps shift cybersecurity from "administrative burden" to "standard of care," especially where digital health is expanding into community and primary-care settings.

Implementation in Nigeria can be pragmatic and scalable. For students, core concepts can be introduced early (privacy, safe authentication, reporting culture), reinforced during clinical rotations (secure prescribing, imaging, laboratory workflows), and assessed through case-based discussions and simulation. For practising clinicians, short modular updates can be integrated into departmental meetings and continuing professional development, focusing on locally relevant risks such as shared accounts, personal devices, and third-party service access. Facilities should also invest in two-way learning: incident reporting should feed back into targeted training, and training outcomes (e.g., phishing simulation results, incident reporting rates, password hygiene compliance) should be monitored and used for improvement.

Nigeria's digital health ambitions will be difficult to sustain if cybersecurity remains siloed within IT departments. Embedding cybersecurity education across health training and practice alongside governance, resilient technology, and realistic incident response supports patient safety, protects public trust, and strengthens the continuity of care during disruptions.

Ethical Declaration and Consent

Not applicable.

Declaration of Conflicting Interests

The authors declare no conflicts of interest.

References

1. Nigeria Digital in Health Initiative. Nigeria Digital in Health Initiative (NDHI). https://www.digitalhealth.gov.ng/ (accessed 20 Feb 2026).

2. World Health Organization. Global strategy on digital health 2020–2025. Geneva: WHO; 2021. https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf (accessed 20 Feb 2026).

3. Argaw ST, Pastoriza JRT, Lacey D, et al. Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. BMC Med Inform Decis Mak. 2020;20(1):146. https://doi.org/10.1186/s12911-020-01161-7

4. Wasserman J. Cybersecurity in hospitals: a systematic, organizational perspective. Front Digit Health. 2022;4:862221. https://doi.org/10.3389/fdgth.2022.862221

5. Monticone DK, Dixon P, Aghili D. Cybersecurity in healthcare: a systematic review of modern threats and trends. Technol Health Care. 2017;25(1):1–10. https://doi.org/10.3233/THC-161263

6. Vartiainen T, et al. Vulnerability to cyberattacks and sociotechnical solutions for health care systems: systematic review. J Med Internet Res. 2024;26:e46904. https://doi.org/10.2196/46904

7. Dameff C, et al. Ransomware attack associated with disruptions at adjacent emergency departments in the US. JAMA Netw Open. 2023;6(5):e2312270. https://doi.org/10.1001/jamanetworkopen.2023.12270

8. Guo WA, et al. Impact of trauma hospital ransomware attack on surgical residency training. J Surg Res. 2018;232:389–397. https://doi.org/10.1016/j.jss.2018.06.072

9. Lehmann CU, et al. Data breach remediation efforts and their implications for hospital quality. Health Serv Res. 2019;54(5):971–980. https://doi.org/10.1111/1475-6773.13203

10. Priestman W, Sridharan S, Vigne H, et al. Phishing in healthcare organisations: threats, mitigation and approaches. BMJ Health Care Inform. 2019;26:e100031. https://doi.org/10.1136/bmjhci-2019-100031

11. Gordon WJ, et al. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. J Am Med Inform Assoc. 2019;26(6):547–552. https://doi.org/10.1093/jamia/ocz005

12. Boyens J, Smith A, Bartol N, et al. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161r1 Update 1). 2024. https://doi.org/10.6028/NIST.SP.800-161r1-upd1

13. Osama M, Ateya AA, Sayed MS, et al. Internet of Medical Things and Healthcare 4.0: Trends, requirements, challenges, and research directions. Sensors. 2023;23(17):7435. https://doi.org/10.3390/s23177435

14. Bonacina S, Dehghantanha A, Choo K-KR, et al. Influence of human factors on cyber security within healthcare organisations: a systematic review. Sensors. 2021;21(15):5119. https://doi.org/10.3390/s21155119

15. Kamerer DB, McDermott D. Cybersecurity: nurses on the front line. J Nurs Regul. 2020;11(1):48–55. https://doi.org/10.1016/S2155-8256(20)30014-4

16. Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. J Med Internet Res. 2018;20(5):e10059. https://doi.org/10.2196/10059

17. National Institute of Standards and Technology (NIST). Cybersecurity Framework (CSF) 2.0. https://www.nist.gov/cyberframework (accessed 20 Feb 2026).

18. Frati F, Braghin C, Riva G, et al. AERAS approach: cybersecurity education and training in cyber ranges for public administrations. Int J Inf Secur. 2024. https://doi.org/10.1007/s10207-023-00802-y

19. Joint Task Force. Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5). 2020. https://doi.org/10.6028/NIST.SP.800-53r5

20. Sreenath SSR, Hewitt B, Sreenath S. Understanding security behaviour among healthcare professionals by comparing results from technology threat avoidance theory and protection motivation theory. Behav Inf Technol. 2024;44(2):181–196. https://doi.org/10.1080/0144929X.2024.2314255

21. Nelson A, Rekhi S, Souppaya M, Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: a CSF 2.0 Community Profile (NIST SP 800-61r3). 2025. https://doi.org/10.6028/NIST.SP.800-61r3

22. Gandhi NS, et al. Ransomware recovery and imaging operations: lessons learned and planning considerations. J Digit Imaging. 2021;34(3):731–740. https://doi.org/10.1007/s10278-021-00466-x

23. Nigeria Data Protection Commission (NDPC). Resources (includes Nigeria Data Protection Act, 2023; Nigeria Data Protection Regulation 2019; and workforce training guidance notices). https://ndpc.gov.ng/resources/ (accessed 20 Feb 2026).

24. Odusote A. Data misuse, data theft and data protection in Nigeria: a call for a more robust and more effective legislation. Beijing Law Review. 2021;12(4):1284–1298. https://doi.org/10.4236/blr.2021.124066