**UNIJERPS**
Unizik Journal of Educational Research and Policy Studies VOL.19 (2);
***January-June, 2025*** https://unijerps.org
***2023 Impact Factor:*** **6.834;** 2022 ***Impact Factor***: 5.156; ***2021 Impact Factor: 5.641;***
***2020 Impact Factor: 5.355.*** *Indexing and Impact Factor URL: http://sjifactor.com/passport.php?id=21363*

# UNDERSTANDING CYBERSECURITY IN THE IMPLEMENTATION OF HEALTH INFORMATION MANAGEMENT SERVICES

**Jacob Kehinde Opele**
Department of Library and Information Science, Federal University Oye-Ekiti, Nigeria
Email: jacob.opele@fuoye.edu.ng

**Babale Garba Nafada**
Aminu Kano Teaching Hospital, Kano, Nigeria
Email: garbanafada@gmail.com

## ABSTRACT
*The increasing digitization of healthcare services in Nigeria has transformed health information management (HIM), enhancing operational efficiency and patient care. However, this transition has also exposed healthcare organizations to significant cybersecurity threats, including malware, phishing attacks, and ransomware. This paper examines the current cybersecurity landscape within Nigeria's healthcare sector, highlighting the various challenges posed by these threats, such as resource limitations and a lack of awareness among healthcare professionals. By emphasizing the necessity of proactive cybersecurity measures, including regular training, investment in advanced technologies, and the adoption of established frameworks, this study aims to provide a comprehensive overview of effective strategies for safeguarding sensitive health information. Furthermore, it explores the critical importance of fostering a culture of cybersecurity awareness among all stakeholders in the healthcare system. The paper concludes by offering actionable recommendations for healthcare organizations to enhance their cybersecurity posture, ensuring the protection of patient data and the continuity of healthcare services in an increasingly digital environment. Ultimately, this research underscores the imperative for a coordinated approach to cybersecurity in Nigeria's healthcare sector, promoting resilience against evolving cyber threats.*

**Keywords:** Cybersecurity, Health Information Management, Nigeria, Digital Health, Cyber Threats, Healthcare Sector

## Introduction
As healthcare systems worldwide increasingly adopt digital solutions, the need for robust cybersecurity measures has never been more pressing. In Nigeria, the shift toward Electronic Medical Records (EMR) and Electronic Health Records (EHR) is reshaping how health information is managed, shared, and protected. However, this transition is accompanied by an alarming rise in cyber threats, necessitating a comprehensive understanding of cybersecurity principles among Health Information Management professionals (Awogbami et al, 2020). As Nigeria advances toward a more digitized healthcare system, the implementation of Health Information Management (HIM) services has become

paramount in enhancing the efficiency and effectiveness of healthcare delivery. The adoption of Electronic Medical Records (EMR) and Electronic Health Records (EHR) has revolutionized data management, enabling healthcare providers to access patient information swiftly and facilitate better clinical decision-making (Awogbami et al, 2020). However, this digital transformation has also introduced significant vulnerabilities, making healthcare organizations prime targets for cybercriminals.

Cybersecurity, defined as the practice of protecting systems, networks, and programs from digital attacks, is crucial in safeguarding sensitive health information (Snigdhya et al., 2024). In Nigeria, where healthcare systems are increasingly interconnected and reliant on technology, the risks associated with inadequate cybersecurity measures have escalated (Adepoju & Opele, 2021). Cyber threats such as ransomware, data breaches, and phishing attacks pose serious risks to patient confidentiality and the integrity of healthcare services. The healthcare sector is particularly vulnerable due to the sensitive nature of the data involved and the potential repercussions of data loss or compromise (Clement et al., 2024).

Despite the growing awareness of cybersecurity threats, many healthcare organizations in Nigeria face challenges in implementing effective cybersecurity strategies. Factors such as limited resources, insufficient training, and a lack of regulatory frameworks contribute to the vulnerability of health information systems (Adepoju & Opele, 2021). For instance, a study highlighted that financial limitations and inadequate ICT resources are significant barriers to the effective implementation of electronic health records in Nigeria (Opele et al., 2019). Furthermore, the cultural perception of cybersecurity often leads to complacency, with organizations prioritizing operational efficiency over robust security measures. This paper explored the critical role of cybersecurity in the implementation of HIM services in Nigeria. By examining the current landscape of cybersecurity threats, best practices, and the unique challenges faced by healthcare organizations, this study seeks to highlight the imperative for a proactive approach to protecting sensitive health information. Ultimately, fostering a culture of cybersecurity awareness and resilience is essential for ensuring the integrity and confidentiality of health data in an increasingly digital healthcare environment.

## The Cybersecurity Landscape in Nigeria

### Current Threats

The Nigerian healthcare sector is increasingly susceptible to a variety of cybersecurity threats that exploit the vulnerabilities inherent in healthcare information systems. Among the most prevalent threats are malware, phishing attacks, and ransomware, each posing unique challenges to the security of health data. Malware is a broad category of malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. In healthcare settings, malware can compromise patient records, disrupt services, and lead to significant operational losses. A report by the

Daniels (2023) indicated a marked increase in malware infections targeting healthcare organizations, highlighting the urgent need for robust defenses. Phishing attacks are another significant threat, characterized by fraudulent attempts to obtain sensitive information by masquerading as trustworthy entities.

Cybercriminals often target healthcare professionals through deceptive emails or messages that appear legitimate, tricking them into providing login credentials or personal information. According to a study by (Singh, et al. 2022). Healthcare workers in Nigeria are frequently targeted by phishing schemes, with many falling victim due to inadequate training and awareness about recognizing such threats. Ransomware, a particularly alarming form of malware, encrypts data and demands payment for the decryption key. The healthcare sector is an attractive target for ransomware attacks because of the critical nature of the data involved. The disruption caused by such attacks can halt patient care, jeopardizing lives and leading to substantial financial losses. A recent incident reported by the Yususf, et al. (2024) detailed a ransomware attack on a major hospital network, resulting in a temporary shutdown of its services and a breach of thousands of patient records. O'Brien, at al. (2024) emphasizes that these threats not only lead to data breaches but can also compromise patient care, as delayed access to medical records or disrupted services can have dire consequences for patient outcomes. The interconnectedness of healthcare systems further exacerbates these threats, as vulnerabilities in one area can lead to widespread repercussions across the network of health services.

**The Need for Awareness**

Despite the critical nature of these cybersecurity threats, there remains a concerning lack of awareness among healthcare professionals in Nigeria regarding the risks associated with inadequate cybersecurity measures. This gap in understanding can lead to complacency, making healthcare organizations even more vulnerable to cyberattacks. Health Information Management (HIM) practitioners play a pivotal role in safeguarding sensitive health data. However, many lack the necessary training and resources to effectively identify and mitigate cybersecurity risks. A survey conducted by Ahmed, (2022) found that a significant percentage of healthcare professionals in Nigeria do not receive formal training in cybersecurity practices, leaving them ill-equipped to recognize potential vulnerabilities within their systems.

As noted by He, Aliyu, Evans, and Luo, C. (2021), the intersection of healthcare and technology necessitates a paradigm shift in how cybersecurity is perceived and addressed. It is imperative for HIM practitioners to be proactive in understanding the evolving cyber threat landscape and to cultivate an organizational culture that prioritizes cybersecurity. This includes not only technical training but also fostering a mindset that recognizes the importance of protecting patient information as a fundamental responsibility. Moreover, awareness initiatives should extend beyond

just HIM professionals to include all healthcare workers, administrative staff, and even patients. Comprehensive training programs that cover the basics of cybersecurity, common threats, and best practices for safeguarding information can empower all stakeholders in the healthcare sector to take an active role in maintaining security. Essentially, enhancing awareness about cybersecurity threats and best practices in the Nigerian healthcare sector is essential for building resilience against cyberattacks. By investing in education and training, healthcare organizations can create a more secure environment for patient data, ultimately improving the safety and quality of healthcare services.

**Key Principles of Cybersecurity in HIM**
**Proactive Measures**
To effectively combat cyber threats, healthcare organizations in Nigeria must adopt a proactive approach to cybersecurity. This includes several key strategies:
**Regular Training and Education:** Continuous professional development is essential for HIM practitioners to stay abreast of the latest threats and best practices. Regular training sessions can equip healthcare staff with the knowledge to recognize potential security threats, understand the importance of data protection, and implement necessary safeguards. A study by Ahmed, (2022) emphasizes that ongoing education in cybersecurity practices significantly enhances the overall security posture of healthcare organizations. Furthermore, simulated phishing exercises can help +staff identify fraudulent communications, thereby reducing the likelihood of successful attacks.
**Investment in Technology:** Utilizing advanced security tools is crucial in mitigating risks associated with cyber threats. Healthcare organizations should invest in comprehensive cybersecurity solutions, including antivirus software, firewalls, encryption tools, and intrusion detection systems. These technologies can help detect and prevent unauthorized access to sensitive health information. Additionally, implementing secure access controls and multi-factor authentication can further protect against data breaches. The Nigerian Cybersecurity Agency (2023) advises that prioritizing technological investments is vital for safeguarding health data in an increasingly digital landscape.
**Collaboration and Information Sharing:** Establishing partnerships between healthcare organizations can foster a culture of shared knowledge and resources to combat cyber threats collectively. Collaborative initiatives, such as information-sharing networks, allow organizations to exchange insights on emerging threats, effective response strategies, and best practices. By working together, organizations can create a more resilient cybersecurity framework that benefits the entire healthcare sector. O'Brien et al. (2024) stresses the importance of collaboration in addressing cybersecurity challenges, particularly in developing countries where resources may be limited.
**Frameworks and Standards:** Implementing established cybersecurity frameworks can guide HIM professionals in developing comprehensive security strategies. The Five Principles of Cybersecurity (5P's)—

protection, detection, response, recovery, and governance—provide a structured approach to safeguarding health information.

- **Protection**: This principle focuses on implementing measures to secure health information from unauthorized access and breaches. This includes employing encryption, access controls, and regular security assessments.
- **Detection**: Organizations must establish effective monitoring systems to detect potential security incidents promptly. This may involve the use of intrusion detection systems and regular audits of access logs.
- **Response**: Developing a clear incident response plan is critical for minimizing the impact of a cybersecurity breach. This plan should outline the steps to take in the event of an incident and designate roles and responsibilities for staff.
- **Recovery**: After a cybersecurity incident, organizations must have a recovery plan that includes restoring systems and data from backups, ensuring continuity of care, and conducting post-incident analysis to improve future responses.
- **Governance**: Effective governance involves establishing policies and procedures that guide cybersecurity efforts across the organization. This includes compliance with relevant regulations and standards, as well as ongoing risk assessments to identify and mitigate vulnerabilities.

**Challenges to Effective Cybersecurity Implementation**

Literature have reported the following challenges affecting effective cybersecurity implementation in health care sector

**Resource Limitations:** One of the most significant barriers to effective cybersecurity in Nigeria's healthcare sector is the lack of resources. Many healthcare organizations operate with limited budgets, making it challenging to invest in necessary cybersecurity infrastructure and training. According to a report by the Nigerian Communications Commission (2022), financial constraints are a primary reason many healthcare facilities cannot implement comprehensive cybersecurity measures. Without adequate funding, organizations may struggle to acquire essential security technologies and may not be able to hire skilled cybersecurity personnel.

**Cultural Attitudes toward Cybersecurity:** There is often a cultural reluctance to prioritize cybersecurity within healthcare organizations. Many stakeholders may view cybersecurity as an IT issue rather than a critical organizational concern. This mindset can lead to complacency, making systems more vulnerable to attacks. Changing this perception is crucial for fostering a security-first culture. Leadership must advocate for the importance of cybersecurity, emphasizing that protecting patient data is a collective responsibility. Educational initiatives and awareness campaigns can help shift this cultural attitude, encouraging all staff members to engage actively in cybersecurity practices.

## Conclusion

The rapid digitization of healthcare services in Nigeria presents significant opportunities for improving patient care and operational efficiency. However, it also exposes the sector to a myriad of cybersecurity threats that can jeopardize the integrity and confidentiality of sensitive health information. As highlighted throughout this paper, the Nigerian healthcare sector faces critical challenges, including increasing cyber threats, a lack of awareness among healthcare professionals, and resource limitations. To protect patient data and ensure the smooth functioning of healthcare services, it is imperative for healthcare organizations to adopt a proactive and comprehensive approach to cybersecurity. By implementing robust security measures, fostering a culture of awareness, and investing in advanced technologies, healthcare organizations can enhance their resilience against cyber threats. Moreover, the adoption of established cybersecurity frameworks will help guide HIM professionals in developing effective security strategies. As the landscape of cybersecurity continues to evolve, so too must the strategies employed by healthcare providers to safeguard sensitive information.

## Recommendations

The following recommendations are suggested for policy and practice

1. Healthcare organizations should invest in regular cybersecurity training for all staff members, including HIM practitioners, to ensure they are equipped with the knowledge to recognize and respond to potential threats. This could involve workshops, online courses, and simulated cyberattack scenarios to improve awareness and response capabilities.
2. Organizations must allocate sufficient resources to acquire and maintain advanced cybersecurity technologies, such as firewalls, intrusion detection systems, and encryption tools. Regular updates and maintenance of these technologies are essential to protect against emerging threats.
3. Establish partnerships with other healthcare organizations and cybersecurity experts to create a network for sharing threat intelligence, best practices, and resources. Collaborative efforts can enhance the overall security posture of the healthcare sector.
4. Organizations should adopt established cybersecurity frameworks, such as the Five Principles of Cybersecurity, to guide their security strategies. This structured approach will help ensure that all aspects of cybersecurity are addressed, from prevention to response and recovery.
5. Leadership must actively promote the importance of cybersecurity across the organization. This includes incorporating cybersecurity into the organizational culture, encouraging staff to take ownership of data protection, and fostering an environment where security concerns can be openly discussed.
6. Engage with government and regulatory bodies to advocate for policies that support cybersecurity initiatives within the healthcare sector. This includes funding for cybersecurity infrastructure, establishing clear regulations, and

providing incentives for organizations to enhance their security measures.

7. Healthcare organizations should perform comprehensive risk assessments to identify vulnerabilities within their systems. Regular audits will help organizations stay ahead of potential threats and adapt their cybersecurity strategies accordingly.

By implementing these recommendations, the Nigerian healthcare sector can significantly improve its cybersecurity posture, ensuring the protection of sensitive health information and the continuity of care for patients. As the digital landscape evolves, a proactive and collaborative approach to cybersecurity will be essential for safeguarding the future of healthcare in Nigeria.

## REFERENCES

Adepoju, E.O & Opele, J. . (2021). Technology Application in Health Information Management in Obafemi Awolowo University Teaching Hospitals Complex (OAUTHC) Ile-Ife, Osun State. *International Journal of Research Publications (IJRP.ORG).*, *74*(1), 17–17.

Adepoju, E. O., & Opele, J. K. (2021). Barriers to Implementing Electronic Health Information Management in Patient Care. *Background. Artic. IOSR J. Res. Method Educ*, 1-24.

Awogbami, P.A., Opele, J.K & Lawal, J. . (2020). Benefits and challenges of using ICTS in health information management at Olabisi Onabanjo University Teaching Hospital, Sagamu, Ogun State, Nigeria. *Journal of Applied Information Science and Technology*, *13*(1), 307–318.

Adepoju, E., & Opele, J.K. (2021). Technology Application in Health Information Management in Obafemi Awolowo University Teaching Hospitals Complex (Oauthc) Ile-Ife, Osun State. *International Journal of Research Publications*, *74*(1), 70–86. https://doi.org/10.47119/ijrp100741420211841

Clement, T., Obunadike, C., Ekweli, D. C., Ejiofor, O. E., Ogunleye, O., Yufenyuy, S. S.& Obunadike, C. J. (2024). Cyber analytics: modelling the factors behind healthcare data breaches for smarter security solutions. *International Journal of Advance Research, Ideas and Innovations in Technology*, *10*(1), 49-75.

Daniels, O. (2023). *National Cybersecurity Policy and Strategy of Nigeria: A Case Study* (Doctoral dissertation, Capitol Technology University).

Ahmed, N. B. (2022). *Cybersecurity in Healthcare System: Evaluation and Assessment of the Cybersecurity readiness of Mobile Field Hospital's Resilience* (Doctoral dissertation, IMT-MINES ALES-IMT-Mines Alès Ecole Mines-Télécom).

He, Y., Aliyu, A., Evans, M., & Luo, C.

(2021). Health care cybersecurity challenges and solutions under the climate of COVID-19: scoping review. *Journal of medical Internet research*, *23*(4), e21747.

O'Brien, N., Crespo, R. F., O'Driscoll, F., Prendergast, M., Chana, D., Darzi, A., & Ghafur, S. (2024). Usability and Feasibility Evaluation of a Web-Based and Offline Cybersecurity Resource for Health Care Organizations (The Essentials of Cybersecurity in Health Care Organizations Framework Resource): Mixed Methods Study. *JMIR Formative Research*, *8*(1), e50968.

Opele, J. K., Omole, M. S., & Adebayo, T. T. (2019). The management of Health Records Libraries through the lens of Ranganathan's theory. *Library Philosophy and Practice (e-Journal).* 3733. https://digitalcommons.unl.edu/libphilprac/3733 .

Singh, I., & Singh, Y. A. S. H. I. K. (2022). Cyber-security knowledge and practice of nurses in private hospitals in northern Durban, kwazulu-Natal. *Journal of Theoretical and Applied Information Technology*, *100*(1), 246-267.

Snigdhya, N. S., Uddin, S., & Dipu, A. (2024). *Integrating Climate Change Adaptation into Flood Risk Management : Global Perspectives*. *X*(8), 177–194. https://doi.org/10.51244/IJRSI

Yusuf, M. K., Danladi, A. J., Shombot, E., Dusserre, G., Odey, V. A., Baba-Ahmed, N. B., & Lawan, M. I. (2024). The Growing Cybersecurity Crisis in Healthcare: A Call to Action. *American Journal of Innovation in Science and Engineering*, *3*(3), 55-68.