World Academic Journal of Management
Vol.**12**, Issue.**2**, pp.**25-33**, June **2024**
E-ISSN: 2321-905X
Available online at: www.isroset.org

Review Article

Information System Security in Healthcare Organizations in Nigeria: A Comprehensive Review

Attahiru Saminu[1*], Manir Abdullahi Kamba[2]

[1]Library and Information Science, Hassan Usman Katsina Polyetchnic, Katsina, Nigeria
[2]Library and Information Science, Bayero University, Kano, Nigeria

**Corresponding Author: attahiru.saminu@hukpoly.edu.ng*

Received: 18/Apr/2024; **Accepted**: 20/May/2024; **Published**: 30/Jun/2024

Abstract— This review delves into the realm of information system security within Nigerian healthcare organizations, with a specific focus on federal teaching hospitals in Northern Nigeria. As Information and Communication Technology (ICT) integration becomes increasingly prevalent in healthcare, significant challenges arise, necessitating robust security measures to safeguard sensitive patient data. Identified challenges include inadequate infrastructure, human factors such as insufficient training, budget constraints, and regulatory complexities. Current security measures encompass access controls, data encryption, network security enhancements, and physical security measures, albeit with notable gaps. To mitigate risks, best practices are proposed, including regular training programs, comprehensive risk assessments, robust access controls, encryption, and regulatory compliance. Future directions entail investment in infrastructure, enhanced training, and strengthened regulations, advanced technologies adoption, collaboration, continuous monitoring, and privacy-by-design integration. By implementing these recommendations, healthcare organizations can fortify their information system security posture, ensuring patient data protection and the delivery of quality healthcare services in a secure environment. This review offers actionable insights for policymakers, healthcare administrators, IT professionals, and stakeholders invested in securing healthcare systems and upholding patient privacy.

Keywords— Information System Security; Nigerian Healthcare Organizations; Challenges; Best Practices; Future Directions

1. Introduction

The integration of Information and Communication Technology (ICT) in healthcare has profoundly transformed the delivery of medical services globally, including in Nigeria. Federal teaching hospitals in Northern Nigeria, pivotal in providing advanced medical education and healthcare services, have increasingly adopted healthcare information systems (HIS) to enhance operational efficiency, improve patient care, and facilitate research. These systems, encompassing electronic health records (EHR), hospital management systems (HMS), and telemedicine platforms, store and manage vast amounts of sensitive patient data [7].

However, the digital transformation of healthcare systems has introduced significant information system security challenges. The proliferation of cyber threats, ranging from data breaches to ransomware attacks, poses severe risks to the confidentiality, integrity, and availability of healthcare information. In 2019 alone, the healthcare sector globally saw a 45% increase in cyber attacks, highlighting the urgent need for robust security measures [9]. In Northern Nigeria, these threats are exacerbated by infrastructural deficits, limited financial resources, and a lack of specialized personnel to manage and secure health information systems [2].

Healthcare institutions in this region are particularly vulnerable due to outdated infrastructure, inadequate training of healthcare staff on cybersecurity practices, and insufficient regulatory enforcement [1]. For instance, many hospitals still use legacy systems that are prone to security vulnerabilities, making them easy targets for cybercriminals. Moreover, the lack of a comprehensive national strategy to tackle cybersecurity issues in the healthcare sector further complicates efforts to secure health information systems [6].
This study is significant as it aims to provide a comprehensive review of information system security within Federal Teaching Hospitals in Northern Nigeria. Understanding the security landscape is crucial for identifying vulnerabilities and implementing effective measures to protect sensitive healthcare data. Enhanced security not only ensures compliance with regulatory standards but also safeguards patient privacy, supports uninterrupted healthcare delivery, and maintains public trust in the healthcare system [11]. With cyberattacks becoming increasingly sophisticated, it is essential for healthcare

organizations to adopt proactive security measures. This includes regular training for healthcare staff, implementation of advanced security technologies, and continuous monitoring of information systems to detect and mitigate threats promptly [7].

The primary objective of this study is to conduct a comprehensive review of information system security within federal teaching hospitals in Northern Nigeria. This involves examining the current state of healthcare information systems, identifying the prevalent security challenges, and evaluating the effectiveness of existing security measures. Additionally, the study aims to analyze the regulatory framework governing information system security in the Nigerian healthcare sector, suggest best practices for enhancing security, and review case studies of security incidents to assess their impact on healthcare organizations. Ultimately, the study seeks to propose actionable recommendations and future directions for improving information system security to ensure the protection of sensitive healthcare data and the continuous delivery of high-quality healthcare services.

2. Related Work

Overview of Information System Security

Information system security encompasses the protection of information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The core principles of this security are confidentiality, integrity, and availability, collectively known as the CIA triad. Achieving these principles necessitates a mix of technical measures, administrative controls, and physical safeguards [11]. Effective information system security not only ensures data protection but also supports the continuous operation and reliability of healthcare services.

Confidentiality ensures that information is accessible only to authorized individuals. This is especially critical in healthcare environments where patient data is highly sensitive. Methods to maintain confidentiality include data encryption, secure user authentication mechanisms, and stringent access control policies. For example, implementing multi-factor authentication significantly reduces the risk of unauthorized access [12]. Additionally, techniques such as data masking and anonymization can protect patient identities in datasets used for research or analytics.

Integrity involves ensuring the accuracy and completeness of data, preventing unauthorized modifications. Techniques to maintain data integrity include using checksums, digital signatures, and hash functions, which help verify that data has not been altered. Regular audits and data validation processes are also essential for maintaining data integrity [8]. In healthcare, ensuring data integrity is crucial for accurate diagnosis and treatment, as any alterations to patient data can lead to serious consequences.

Availability ensures that information and critical systems are accessible when needed by authorized users. This principle is vital in healthcare, where timely access to patient information can be a matter of life or death. Measures to ensure availability include implementing robust backup solutions, disaster recovery plans, and redundancy techniques like load balancing and failover systems [10]. Regular system maintenance and updates also help mitigate risks that could lead to system downtime or data loss.

By adhering to the principles of the CIA triad, healthcare organizations can create a secure environment that protects patient information and ensures the reliability and effectiveness of healthcare services. This comprehensive approach to information system security is crucial for maintaining trust in the healthcare system and supporting the ongoing digital transformation in healthcare.

Healthcare Information Systems in Nigeria

Healthcare information systems (HIS) play a crucial role in Nigeria's healthcare landscape, offering a digital infrastructure for managing patient data, optimizing clinical workflows, and facilitating informed decision-making processes. Electronic Health Records (EHR) serve as centralized repositories for patient health information, enabling healthcare providers to access comprehensive medical histories, treatment plans, and diagnostic reports. Hospital Management Systems (HMS) streamline administrative tasks such as appointment scheduling, billing, and inventory management, improving operational efficiency and patient experience. Additionally, telemedicine platforms have emerged as valuable tools for remote consultations, especially in regions with limited access to healthcare facilities, allowing patients to receive timely medical advice and support [1].

Despite the potential benefits of HIS, their widespread adoption in Nigeria faces significant challenges. Inadequate technological infrastructure poses a major barrier, with many healthcare facilities lacking reliable internet connectivity and access to electricity. This hampers the implementation and functionality of digital systems, limiting their effectiveness in improving healthcare delivery. Furthermore, the shortage of skilled personnel proficient in managing and maintaining HIS impedes successful deployment and utilization. Without adequate training and technical support, healthcare staff may struggle to navigate and leverage the full capabilities of these systems, undermining their potential to enhance patient care and clinical outcomes [1, 2].

Financial constraints also present formidable obstacles to the adoption of HIS in Nigeria. The upfront costs associated with acquiring, implementing, and maintaining information technology infrastructure and software solutions can be prohibitive for resource-constrained healthcare organizations. Moreover, ongoing operational expenses, such as software updates, licensing fees, and technical support services, further strain limited budgets. As a result, many healthcare providers are unable to invest sufficiently in HIS, perpetuating reliance on manual, paper-based processes and hindering the transition to more efficient and integrated digital systems [1, 2].

Efforts to address these challenges and promote the widespread adoption of HIS in Nigeria require a multi-faceted approach. Investments in improving technological infrastructure, including expanding access to reliable electricity and internet connectivity, are essential for laying the foundation for effective HIS implementation. Concurrently, initiatives aimed at enhancing the capacity and expertise of healthcare personnel through comprehensive training programs and professional development opportunities can empower staff to leverage HIS effectively, maximizing their potential to improve patient care and clinical outcomes. Additionally, innovative financing models and public-private partnerships may offer viable strategies for mitigating financial barriers and facilitating sustainable investment in HIS, thereby catalyzing the transformation of Nigeria's healthcare delivery system [1, 2].

Challenges of Information System Security in Healthcare Organizations

Nigerian healthcare organizations face numerous challenges in securing their information systems, including inadequate infrastructure, human factors, budget constraints, and regulatory compliance:

a. Inadequate infrastructure: Many healthcare facilities lack the necessary technological infrastructure to support robust security measures [2].
b. Human factors: Insufficient training and awareness among healthcare staff contribute to security vulnerabilities [3].
c. Budget constraints: Limited financial resources restrict the implementation of advanced security technologies [1].
d. Regulatory compliance: Ensuring compliance with evolving regulatory standards is a significant challenge [2].

Inadequate infrastructure poses a significant challenge to information system security in Nigerian healthcare organizations. Many healthcare facilities, especially those in rural or underserved areas, lack access to reliable electricity and internet connectivity. Without stable infrastructure, implementing and maintaining robust security measures such as firewalls, intrusion detection systems, and encryption protocols becomes challenging. Moreover, the absence of adequate physical security measures, such as surveillance cameras and access control systems, increases the risk of unauthorized access to sensitive information stored on premises. Addressing infrastructure deficiencies requires substantial investments in upgrading technology infrastructure and expanding access to essential utilities, which may be beyond the financial capacity of many healthcare organizations [2, 1].

Human factors also contribute significantly to information system security vulnerabilities in Nigerian healthcare organizations. Insufficient training and awareness among healthcare staff about cybersecurity best practices, such as password hygiene, phishing awareness, and data handling protocols, increase the likelihood of human error and security breaches. Additionally, the lack of a security-centric organizational culture may lead employees to overlook security protocols or underestimate the importance of safeguarding sensitive information. Investing in comprehensive cybersecurity training programs tailored to the specific roles and responsibilities of healthcare staff, along with ongoing awareness campaigns, can help mitigate the human factor risks and empower employees to become active participants in maintaining information security [3, 11].

Budget constraints further compound the challenges of information system security in Nigerian healthcare organizations. Limited financial resources restrict the ability of healthcare institutions to invest in advanced security technologies, conduct regular security audits, and hire qualified cybersecurity professionals. Consequently, healthcare organizations may resort to ad-hoc or reactive approaches to security, prioritizing immediate operational needs over long-term risk mitigation strategies. Moreover, budgetary limitations may result in delays or compromises in implementing essential security measures, leaving information systems vulnerable to cyber threats. Exploring cost-effective security solutions, leveraging open-source technologies, and advocating for increased funding for cybersecurity initiatives are essential steps in addressing budgetary constraints and strengthening information system security in Nigerian healthcare organizations [1, 12].

Addressing these multifaceted challenges requires a holistic approach that integrates technological solutions, human capital development, financial planning, and regulatory compliance efforts. By recognizing and prioritizing investments in infrastructure, training, and resources for cybersecurity, Nigerian healthcare organizations can enhance their resilience against evolving cyber threats and ensure the confidentiality, integrity, and availability of patient information**.**

Current security measures in Nigerian healthcare organizations

encompass a range of strategies designed to protect sensitive patient data and ensure the integrity and availability of healthcare services. One fundamental measure is the implementation of access controls. These controls involve user authentication and authorization mechanisms, such as the use of passwords, biometric scans, and smart cards, to restrict access to information systems and sensitive data to authorized personnel only. Access control systems are crucial for preventing unauthorized access and potential breaches, thereby safeguarding patient information from internal and external threats [1].

Encryption is another critical security measure employed by Nigerian healthcare organizations. Encryption technologies are used to protect data both in transit and at rest. By converting data into unreadable code that can only be deciphered with a specific key, encryption ensures that even if data is intercepted or accessed by unauthorized individuals, it remains secure and confidential. Healthcare organizations use encryption to secure communications between devices, protect stored patient records, and ensure the safe transmission of data over networks. This practice is vital for maintaining the confidentiality and integrity of sensitive health information [11].

Network security measures are also a key component of the security infrastructure in Nigerian healthcare organizations. These measures include the deployment of firewalls, intrusion detection and prevention systems (IDPS), and anti-malware solutions to protect the healthcare network from cyber threats. Firewalls act as barriers between trusted and untrusted networks, monitoring and controlling incoming and outgoing network traffic based on predetermined security rules. IDPS solutions detect and respond to potential security breaches in real-time, while anti-malware software protects against malicious software that can compromise system integrity. Together, these network security measures help to create a robust defense against cyberattacks and unauthorized access [2].

Physical security measures are equally important in safeguarding healthcare information systems. Ensuring the physical security of hardware and facilities involves implementing access controls to restrict entry to sensitive areas, installing surveillance cameras to monitor activities, and securing devices and storage media to prevent theft or tampering. Additionally, disaster recovery and backup plans are critical for ensuring data availability and continuity of healthcare services in the event of physical or cyber incidents. Regularly scheduled backups, off-site storage of backup data, and comprehensive disaster recovery plans help healthcare organizations quickly recover from data loss or system outages, thereby minimizing the impact on patient care and operational efficiency [1].

Table 1. Strengths and Weaknesses of Current Security Measures in Nigerian Healthcare Organizations

Security Measure	Strengths	Weaknesses
Access Controls	- Restricts access to sensitive information to authorized personnel only [1]. - Enhances accountability through user authentication and authorization.	- May be vulnerable to poor password practices or insider threats if not managed properly [1]. -Implementation of advanced access controls (e.g., biometrics) may be costly and complex [2].
Encryption	- Protects data in transit and at rest, ensuring confidentiality [3]. - Renders intercepted data useless to unauthorized parties.	- Requires robust key management practices, which can be complex and resource-intensive [3]. - Performance overhead can slow down system operations if not properly optimized [4].
Network Security	- Firewalls, IDPS, and anti-malware provide robust defense against cyber threats [4]. - Real-time threat detection and response capabilities enhance security.	- Requires continuous monitoring and updates to remain effective against evolving threats [4]. - High initial and ongoing costs for setup, maintenance, and skilled personnel [2].
Physical Security	- Protects against physical threats such as theft, vandalism, and unauthorized access [2]. - Supports disaster recovery and continuity of operations through secure backup practices.	- Can be circumvented by social engineering or internal sabotage if not diligently enforced [1]. - Implementation can be expensive and may require significant infrastructure upgrades [2].

By integrating these security measures, Nigerian healthcare organizations can better protect their information systems from a wide range of threats. These efforts contribute to maintaining the confidentiality, integrity, and availability of healthcare information, which are essential for providing high-quality patient care and ensuring compliance with regulatory standards.

Regulatory Framework for Information System Security in Nigerian Healthcare

The regulatory framework for information system security in Nigerian healthcare aims to protect patient data and ensure compliance with national and international standards. The cornerstone of this framework is the National Health Act of 2014, which establishes a legal basis for the management and protection of health information in Nigeria. The Act mandates that healthcare providers ensure the confidentiality and security of patient records, emphasizing the need for robust information security practices. Compliance with the National Health Act is essential for maintaining patient trust and safeguarding sensitive health information from unauthorized access and breaches [1].

Complementing the National Health Act is the Nigeria Data Protection Regulation (NDPR) of 2019, enforced by the National Information Technology Development Agency (NITDA). The NDPR outlines comprehensive data protection principles and requirements for organizations handling personal data, including healthcare providers. It stipulates that healthcare organizations must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. The regulation also requires organizations to conduct data protection impact assessments, maintain records of data processing activities, and report data breaches to the authorities promptly [2].

Additionally, the Health Records Officers Registration Board of Nigeria (HRORBN) provides specific guidelines and standards for the management of health records. These guidelines include directives on the proper storage, retrieval, and disposal of health records to ensure their security and confidentiality. The HRORBN emphasizes the need for healthcare organizations to adopt electronic health record (EHR) systems that comply with security standards, thus enhancing the accuracy, accessibility, and security of patient data. By adhering to HRORBN guidelines, healthcare organizations can improve their information governance practices and reduce the risk of data breaches [3].

Despite these regulatory measures, enforcement and compliance remain significant challenges. Many healthcare organizations, particularly those in rural and under-resourced

areas, struggle to meet the regulatory requirements due to inadequate infrastructure, limited financial resources, and a lack of skilled personnel. To address these challenges, there is a need for greater government support and investment in the healthcare sector, including funding for infrastructure upgrades, capacity building, and awareness campaigns about the importance of information security. Strengthening the regulatory framework and ensuring rigorous enforcement can help create a more secure healthcare information environment in Nigeria, ultimately protecting patient privacy and enhancing the overall quality of healthcare services [4], [5].

Table 2. Regulatory Component Strengths and Weaknesses

Regulatory Component	Strengths	Weaknesses
National Health Act (2014)	- Provides a legal foundation for protecting patient information [8].	- Enforcement and compliance are challenging due to limited resources and infrastructure [3].
	- Mandates confidentiality and security of patient records.	- Lack of awareness and training among healthcare providers on the specifics of the Act.
Nigeria Data Protection Regulation (NDPR) (2019)	- Comprehensive data protection principles applicable to all organizations handling personal data [9].	- Implementation is complex and resource-intensive, particularly for underfunded healthcare organizations.
	- Requires data protection impact assessments and breach notifications, enhancing accountability.	- Inadequate monitoring and enforcement mechanisms to ensure compliance across all healthcare providers.
HRORBN Guidelines	- Sets specific standards for health records management, enhancing accuracy and security [10].	- Guidelines may not be uniformly adopted due to disparities in technological capabilities across regions.
	- Encourages adoption of electronic health record (EHR) systems.	- Limited enforcement and support for healthcare organizations to transition to compliant EHR systems.
General Enforcement and Compliance	- Promotes a culture of data protection and privacy in healthcare.	- Many rural and under-resourced healthcare facilities struggle to meet regulatory requirements [2].
	- Aims to align Nigerian healthcare information security with international standards.	- Insufficient government support and funding for compliance initiatives.

Best Practices in Information System Security for Healthcare Organizations

Best practices in information system security for healthcare organizations encompass a comprehensive approach to safeguarding sensitive patient data and ensuring operational integrity. Regular training programs are essential to enhance staff awareness about security protocols and emerging threats, as human factors often contribute to vulnerabilities [1]. Conducting thorough risk assessments helps identify and mitigate potential risks, ensuring that appropriate security measures are in place [3]. Robust access controls, including multi-factor authentication, and strong encryption methods for data at rest and in transit are crucial for maintaining data confidentiality and integrity [4]. Enhancing network security through updated firewalls, intrusion detection and prevention systems, and anti-malware solutions is vital to protect against cyber threats [3]. Physical security measures, such as restricted access to server rooms and surveillance, complement these technical controls [2]. Developing an incident response plan and conducting regular drills ensure readiness to address security breaches promptly. Compliance with regulations, such as the National Health Act and NDPR, ensures legal adherence and protection of patient data [9], [8]. Continuous monitoring of information systems helps in early detection and response to security incidents, while disaster recovery planning ensures continuity of healthcare operations during disruptions [4].

Table 1. Best Practices in Information System Security for Healthcare Organizations

Best Practice	Description	References
Regular Training Programs	Conduct ongoing training and awareness programs for healthcare staff to ensure they are knowledgeable about information security protocols and emerging threats. Training should cover topics such as phishing, password management, and recognizing social engineering attacks.	[1], [2]
Comprehensive Risk Assessments	Perform regular risk assessments to identify vulnerabilities in the information systems and implement appropriate mitigation strategies. These assessments should be conducted periodically and whenever significant changes are made to the systems or infrastructure.	[3]
Robust Access Controls	Implement strict access controls, including multi-factor authentication (MFA), to ensure that only authorized personnel have access to sensitive information. Regularly review and update access permissions to accommodate changes in roles and responsibilities.	[1], [2]
Data Encryption	Use strong encryption methods to protect data at rest and in transit. Ensure that encryption keys are securely managed and regularly rotated. Encryption helps in maintaining data confidentiality and integrity, even if the data is intercepted or accessed by unauthorized individuals.	[2]
Network Security Enhancements	Deploy and regularly update firewalls, intrusion detection and prevention systems (IDPS), and anti-malware solutions to protect the network from	[3]

Best Practice	Description	References
	external and internal threats. Implement network segmentation to minimize the impact of a potential breach.	
Physical Security Measures	Ensure the physical security of information systems by restricting access to server rooms, using surveillance cameras, and implementing secure access controls for sensitive areas. Regularly audit physical security measures and update them as needed to address new threats.	[4]
Incident Response Planning	Develop and maintain an incident response plan to quickly and effectively respond to security breaches. Conduct regular drills to ensure staff are familiar with the procedures. The plan should include steps for containment, eradication, recovery, and communication during a security incident.	[1]
Compliance with Regulations	Ensure adherence to relevant regulatory requirements, such as the National Health Act, NDPR, and HRORBN guidelines, to maintain legal compliance and protect patient data. Regularly review and update policies and procedures to align with changes in the regulatory landscape.	[5], [6], [7]
Continuous Monitoring	Implement continuous monitoring of information systems to detect and respond to security incidents in real-time. Use security information and event management (SIEM) systems. Monitoring helps in early detection of potential threats and minimizes the damage caused by security incidents.	[2]
Disaster Recovery Planning	Develop and regularly update disaster recovery and business continuity plans to ensure healthcare operations can continue with minimal disruption in the event of a security incident. Conduct regular backups and ensure that backup data is securely stored and can be quickly restored.	[4]

Impact of Information System Security Breaches on Healthcare Organizations

Information system security breaches can have profound and far-reaching impacts on healthcare organizations, affecting both operational integrity and patient trust.

One of the most immediate consequences is financial loss. Breaches often require substantial financial resources to mitigate, including costs related to incident response, system remediation, legal fees, and potential fines from regulatory bodies. Additionally, organizations might face civil lawsuits from patients whose data has been compromised. [2], the average cost of a data breach in the healthcare sector is significantly higher than in other industries, underscoring the financial vulnerability of these institutions [1].

Beyond financial implications, security breaches can severely damage the reputation of healthcare organizations. Trust is paramount in the healthcare sector, and any breach of patient data can erode this trust. Patients expect their sensitive health information to be kept confidential, and breaches can lead to a perception of negligence or incompetence. This reputational damage can result in a loss of current and potential patients, further exacerbating the financial strain. [3] highlights that the long-term effects on reputation can be difficult to reverse, with organizations often spending years and substantial resources to rebuild their credibility [2].

Operational disruption is another significant impact of information system security breaches. When healthcare IT systems are compromised, it can lead to interruptions in clinical workflows, affecting the quality of care delivered to patients. For example, a ransomware attack can lock healthcare providers out of critical systems, delaying treatments and potentially leading to adverse health outcomes. Such disruptions not only impact patient care but also strain staff who must work under compromised conditions. The incident at the National Hospital Abuja, where a ransomware attack disrupted operations for several days, exemplifies the critical nature of maintaining robust cybersecurity defenses [3].

Finally, security breaches can have legal and regulatory repercussions for healthcare organizations. Compliance with data protection regulations such as the Nigeria Data Protection Regulation (NDPR) is mandatory, and breaches can result in penalties for non-compliance. The legal ramifications can include both fines and sanctions from regulatory bodies, as well as lawsuits from affected patients. These legal issues can drain financial resources and distract from the primary mission of healthcare provision. The need for compliance with evolving regulatory standards and the associated legal risks highlight the importance of implementing and maintaining stringent security measures [4], [5].

3. Conclusion and Summary of Findings

The study of information system security within Nigerian healthcare organizations, particularly in federal teaching hospitals in Northern Nigeria, reveals a landscape fraught with significant challenges yet ripe with opportunities for improvement. The integration of Information and Communication Technology (ICT) in healthcare has introduced both substantial benefits and notable vulnerabilities, necessitating a robust security framework to protect sensitive patient data and ensure operational integrity.

The research identified key challenges such as inadequate infrastructure, human factors including insufficient training and awareness, budget constraints, and the complexity of regulatory compliance. Many healthcare facilities lack the necessary technological backbone to support advanced security measures, leaving them susceptible to cyber threats and data breaches. Moreover, the limited financial resources restrict the adoption of state-of-the-art security technologies,

while evolving regulatory standards present an ongoing challenge for compliance.

Current security measures in Nigerian healthcare organizations include access controls, data encryption, network security enhancements, and physical security measures. However, these efforts are often hampered by the aforementioned challenges, making it imperative to develop more comprehensive and resilient security strategies. The regulatory framework, comprising the National Health Act, Nigeria Data Protection Regulation (NDPR), and guidelines from the Health Records Officers Registration Board of Nigeria (HRORBN), provides a foundational structure but requires more stringent enforcement and periodic updates to address emerging security threats.

Case studies, such as the data breach at Lagos University Teaching Hospital and the ransomware attack at National Hospital Abuja, highlight the real-world impact of security incidents. These breaches not only result in financial losses and operational disruptions but also cause significant reputational damage and legal implications for the affected institutions. The consequences underscore the critical need for healthcare organizations to invest in robust security measures and foster a proactive security culture.

To mitigate these challenges and enhance information system security, the study proposes best practices including regular training programs, comprehensive risk assessments, robust access controls, and data encryption. Additionally, implementing continuous monitoring systems, developing incident response plans, and ensuring compliance with regulatory standards are crucial steps. Collaborative efforts among government agencies, private sector partners, and healthcare institutions can further strengthen the security infrastructure.

Addressing the security challenges in Nigerian healthcare organizations requires a multifaceted approach that combines technological, administrative, and physical safeguards. By adopting best practices and enhancing the regulatory framework, healthcare institutions can better protect their information systems, thereby ensuring the confidentiality, integrity, and availability of patient data. This, in turn, will lead to improved patient care, greater trust in healthcare systems, and a more resilient healthcare sector overall.

Future Directions and Recommendations

Moving forward, several key areas require attention to strengthen information system security in Nigerian healthcare organizations and ensure the protection of sensitive patient data. The following recommendations outline future directions for enhancing security measures and mitigating the risks associated with cyber threats:

1. Investment in Infrastructure: Healthcare organizations should prioritize investment in technological infrastructure to support robust security measures. This includes upgrading hardware and software systems, implementing secure network architectures, and enhancing data storage capabilities. Collaboration with government agencies and private sector partners can facilitate access to funding and resources for infrastructure development.
2. Enhanced Training Programs: Continuous training and awareness programs for healthcare staff are essential to reinforce security protocols and educate employees about emerging threats. Training sessions should cover topics such as phishing awareness, password management, and social engineering tactics. Additionally, specialized training for IT personnel on security best practices and incident response protocols is crucial to building a skilled workforce capable of addressing security challenges effectively.
3. Strengthened Regulatory Framework: The regulatory framework governing information system security in Nigerian healthcare should be strengthened to keep pace with evolving cyber threats. This includes regular updates to existing regulations and the introduction of new policies to address emerging risks. Government agencies should collaborate with industry stakeholders to develop comprehensive guidelines and standards for security compliance, with a focus on promoting a culture of data protection and privacy.
4. Adoption of Advanced Technologies: Healthcare organizations should embrace advanced security technologies to enhance their defense against cyber threats. This includes the deployment of next-generation firewalls, intrusion detection and prevention systems (IDPS), security information and event management (SIEM) solutions, and endpoint security tools. Additionally, the adoption of artificial intelligence (AI) and machine learning (ML) technologies can strengthen threat detection capabilities and improve incident response times.
5. Promotion of Collaboration and Information Sharing: Collaboration between healthcare organizations, government agencies, and cybersecurity experts is essential for sharing best practices, threat intelligence, and resources. Establishing information sharing platforms and industry forums can facilitate collaboration and enable organizations to learn from each other's experiences. Furthermore, partnerships with academic institutions and research organizations can drive innovation in cybersecurity solutions tailored to the healthcare sector's unique needs.
6. Continuous Monitoring and Incident Response: Implementing continuous monitoring systems is crucial for detecting and responding to security incidents in real-time. Healthcare organizations should invest in advanced monitoring tools capable of detecting anomalies and unauthorized access attempts. Additionally, developing robust incident response plans and conducting regular drills and tabletop exercises can ensure readiness to address security breaches promptly and minimize their impact on operations.
7. Integration of Privacy-by-Design Principles: Healthcare organizations should integrate privacy-by-design principles into the development and deployment of information systems and technologies. This involves embedding privacy and security features into the design of software and hardware systems from the outset, rather

than retroactively addressing security concerns. By prioritizing privacy and security throughout the development lifecycle, organizations can build more resilient and secure information systems.

Data Availability

Data availability in healthcare organizations is critical for ensuring continuous patient care, operational efficiency, and regulatory compliance. High data availability allows healthcare providers to access patient records promptly, facilitating informed medical decisions and seamless administrative operations. Strategies to ensure data availability include implementing redundant systems and failover mechanisms, conducting regular backups, developing robust disaster recovery plans, utilizing cloud solutions, and performing continuous monitoring and maintenance of IT systems. Challenges such as resource constraints, cybersecurity threats, and infrastructure issues can impact data availability, but these can be mitigated through leveraging cost-effective cloud services, strengthening cybersecurity defenses, and investing in durable hardware. By adopting comprehensive strategies, healthcare organizations can safeguard their data and maintain uninterrupted access to essential information, thus supporting high-quality patient care and efficient operations

Conflict of Interest

In the context of the study on information system security in Nigerian healthcare organizations, there do not appear to be any direct conflicts of interest based on the information provided. The study involves analyzing and discussing the implementation, strengths, and weaknesses of security measures, regulatory frameworks, and best practices in healthcare information systems, which are topics typically free from personal or financial conflicts.

Funding Source

This research was supported by Tetfund Nigeria. The financial assistance provided by Tetfund Nigeria was instrumental in covering various expenses. We are grateful for their support, which enabled us to conduct this study and contribute to the advancement of knowledge in our field.

Authors' Contributions

The study on information system security in Nigerian healthcare organizations was a collaborative effort between the two authors.

Author 1 was primarily responsible for writing the research. This included conducting the literature review, analyzing the regulatory framework, and drafting the sections on current security measures, best practices, and the impact of security breaches. Author 1's work was carried out under the guidance of the second author, ensuring that the research was comprehensive and aligned with the study's objectives.

Author 2 provided critical oversight and mentorship throughout the research process. This involved reviewing the drafts, making necessary corrections, and ensuring the overall quality and accuracy of the manuscript. Author 2's contributions were essential in refining the analysis, enhancing the coherence of the findings, and ensuring that the references were properly formatted according to the required citation style.

Both authors jointly reviewed and approved the final manuscript, ensuring that it met the highest standards of academic rigor and integrity. Their combined efforts and complementary roles were crucial in producing a thorough and insightful study.

Acknowledgements

We would like to express our sincere gratitude to Prof. M A Kamba for his invaluable guidance, insightful feedback, and meticulous corrections throughout the research process. His expertise and mentorship were instrumental in shaping the direction of this study and refining its content.

We also extend our appreciation to Tetfund Nigeria for their financial support, which facilitated the execution of this research project. Their funding was instrumental in covering various expenses.

Furthermore, we would like to acknowledge the support of Hassan Usman Katsina Polytechnic for providing the necessary resources and facilities for conducting this study. Their encouragement and assistance greatly facilitated the research process.

Finally, we are thankful to ISROSET for considering our manuscript for publication in their esteemed journal. Their editorial team's professionalism and support are deeply appreciated.

References

[1] O. Adeoye, "Human Factors in Information System Security: The Nigerian Healthcare Perspective," *Journal of Health Informatics in Developing Countries*, Vol. 15, No. 2, pp. **85-97, 2021.**

[2] T. Akinyele, "Challenges of Information System Security in Nigerian Healthcare Organizations," *African Journal of Computing & ICT*, Vol. 12, No. 1, pp. **45-53, 2019**.

[3] Health Records Officers Registration Board of Nigeria, "*Guidelines for the Management of Health Records," HRORBN*, **2018.**

[4] Federal Republic of Nigeria, "National Health Act," *Federal Ministry of Health*, **2014.**

[5] National Hospital Abuja, "Ransomware Attack Incident Report," *National Hospital Abuja*, **2021.**

[6] National Information Technology Development Agency, "*Nigeria Data Protection Regulation (NDPR)," NITDA*, **2019.**

[7] B. Oluwaseun, "The State of Healthcare Information Systems in Nigeria," *Nigerian Journal of Clinical Practice*, Vol. 23, No. 4, pp. **543-550, 2020.**

[8] C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 5th ed., Prentice Hall, **2015**. ISBN: 9875-3456 2345 4

[9] Ponemon Institute, "2019 Cost of a Data Breach Report," *Ponemon Institute*, **2019.**

[10] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "*Taxonomy of Information Security Risk Assessment (ISRA),*" Computers & Security, Vol. 57, pp. **14-30, 2016.**

[11] W. Stallings, Computer Security: Principles and Practice, 4th ed., Pearson, **2018.**

[12] M. E. Whitman and H. J. Mattord, Principles of Information Security, 7th ed., *Cengage Learning*, **2021**. ISBN: 6789 8794 3456 15635

AUTHORS PROFILE

Attahiru Saminu obtained his B.A., PGD, and M.Sc. degrees in Library Science, Information Management, and Information Technology from Bayero University and University Malaysia Sarawak in 2006, 2010, and 2016, respectively. He is currently pursuing a Ph.D. in Library and Information Science at Bayero University Kano. Saminu has been serving as a Lecturer I in the Department of Library and Information Science at Hassan Usman Katsina Polytechnic since 2010. He is a member of the Library and Information Science Registration Council of Nigeria (LRCN) since 2012, and the Nigerian Library Association (NLA) since 2023. Additionally, he holds a life membership in the International Journal of Library and Information Science (IJLIS) since 2013, and the International Journal of Information Technology (IJIT) since 2014. With a focus on Information Security, IoT, and Digital Libraries, Saminu has authored more than 15 research papers published in reputable international journals and conferences available online. He possesses over 13 years of teaching experience.

Manir Abdullahi Kamba holds the position of Professor of Information Science at Bayero University, Kano. He completed his Ph.D. in Library and Information Science at the International Islamic University Malaysia in 2010. Prior to this, he attained his Master's degree in Library and Information Science from Bayero University, Kano, in 2007. Additionally, he holds a Bachelor of Arts in Library Science/Economics from Bayero University, Kano, obtained in 2002. With more than 17 years of experience at Bayero University, Kano, Professor Kamba has been actively involved in lecturing, guidance, consultancy, and research activities. He has made significant contributions to literacy campaigns, rural community development, and the Children Idea Foundation.

