SIAR-Global Journal of Computer, Information & Library Science
www.siarpublications.org
info@siarpublications.org Vol. 1 Issue 1 Sept.-Oct. 2025
Global Office **South Africa:** 16 Park Ave, Modderfontein, Johannesburg

Assessment of Compliance With data Protection and Privacy Regulations in the Nigeria Healthcare Sector

K.C. Anyanwu[1], U.M. Mbanaso[2], T.K. Anyachebelu[3], S.E. Chaku[4]

[1,2,3&4]Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria.

Corresponding author email: u.m.mbanaso@nsuk.edu.ng

Abstract

Digitalization in healthcare has expanded the collection, storage, and sharing of patient information, thereby increasing exposure to privacy and data protection risks. In Nigeria, compliance expectations for personal data processing in healthcare are shaped by an evolving regulatory framework, anchored on the Nigeria Data Protection Act (NDPA) 2023 and implementation guidance under the General Application and Implementation Directive (GAID) 2025, alongside sector-specific confidentiality obligations. This study examined awareness levels and reported compliance-related practices in four selected Nigerian healthcare facilities. A cross-sectional quantitative survey was conducted using a structured questionnaire administered to 100 participants comprising patients and healthcare staff. Thirty-eight (38) valid responses were analyzed using descriptive statistical techniques. Spearman's rank correlation was applied as an exploratory test of association for selected ordinal indicators based on complete-case data. Findings revealed uneven awareness of data protection regulations among respondents (n=38), with 37% reporting full awareness and 13% reporting no awareness. Reported safeguards for protecting personal data during storage and transfer (valid n=14) were mainly limited to secure networks (29%) and encryption (21%); several controls, including audit trails/logging, secure disposal, data retention policies, and vendor or third-party security practices, were not identified by respondents.-Among healthcare workers only (n=19), 37% reported being unaware of any incident response plan for data breach events. Key perceived barriers to compliance (valid n=17) included lack of awareness (71%), insufficient resources (53%), rapid technological change (47%), and third-party risks (41.1%). Exploratory correlations based on complete cases (n=11) indicated a positive association between monitoring and adherence (ρ=0.656) and a weak negative association between awareness activities and adherence (ρ=−0.244).

Keywords: Data Protection; Data Privacy; Personal Data; Patient Data; Nigeria Data Protection Act (NDPA) 2023; General Application and Implementation Directive (GAID) 2025; Healthcare; Compliance.

1. INTRODUCTION

Data protection and privacy have become central concerns in today's data-driven world, especially within healthcare environments where large volumes of sensitive personal health information are routinely collected, stored, shared, and processed. Data protection refers to the legal and operational frameworks designed to ensure the secure collection, storage, processing, and sharing of personal data, safeguarding it from misuse, unauthorized access, or breaches (European Union, 2016). Data privacy, meanwhile, refers to an individual's right to control how their personal information is accessed, used, and disclosed (Solove, 2009). These concepts are closely linked and remain central to trust, accountability, and the ethical handling of personal health information in clinical settings. Globally, legislative frameworks such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) have shaped expectations for lawful processing, confidentiality, and individual rights in personal data governance (European Union, 2016; U.S. Congress, 1996). However, research continues to show substantial disparities in interpretation, enforcement capacity, institutional readiness, and technological preparedness across regions, with these gaps often more visible in low-resource and developing contexts (Conduah et al., 2025; Keshta and Odeh 2020). In healthcare, such disparities matter because breaches involving health records can erode patient trust, compromise care continuity, and expose institutions to legal and ethical consequences. Major incidents in other jurisdictions, including the Anthem breach and the American Medical Collection Agency (AMCA) breach, demonstrate the scale and sensitivity of health data risks when governance and security controls are inadequate (Mathews, 2015; Office for Civil Rights, 2018; The HIPAA Journal, 2021). As electronic health records and digital health platforms increase the ease with which information is accessed and shared among stakeholders, privacy and security concerns become even more consequential in protecting patient confidentiality Keshta and Odeh 2020).

In Nigeria, these challenges are amplified by uneven implementation capacity, infrastructure limitations, and varying levels of awareness among healthcare workers and institutions (Idoko, Alakwe, Ugwu, & Idoko, 2024). While Nigeria previously relied heavily on the Nigeria Data Protection Regulation (NDPR) and related guidance (NITDA, 2019), the legal and institutional environment has evolved. The Nigeria Data Protection Act (NDPA) 2023 now provides the primary statutory framework for personal data governance, and the Nigeria Data Protection Commission's General Application and Implementation Directive (GAID) 2025 provides further implementation guidance across sectors (Nigeria Data Protection Act, 2023; Nigeria Data Protection Commission, 2025). In parallel, sector-specific obligations relating to confidentiality and healthcare governance also exist under instruments such as the National Health Act (Federal Government of Nigeria, 2014). Despite these frameworks, the effectiveness of data protection in Nigeria is often constrained by weak enforcement mechanisms and limited regulatory capacity, creating a gap between legal expectations and routine institutional practice (Aloamaka, 2023; Imoisi & Ottah, 2025). This implementation gap is not only a legal issue but also an operational one that becomes more pressing as digital connectivity expands. Broader indicators of regulatory compliance and reporting challenges across Nigeria's digital ecosystem suggest that enforcement capacity and compliance culture may remain uneven, which can indirectly heighten privacy risks for sensitive domains such as healthcare (Nigerian Communications Commission [NCC], 2023). As healthcare organizations increasingly depend on networked systems and external service providers for data storage, communication, and processing, governance weaknesses can translate into practical vulnerabilities in areas such as access control, monitoring, breach readiness, and third-party risk management.

Against this background, this study assesses prevailing knowledge, reported safeguards, and perceived compliance practices relating to data protection and privacy among healthcare stakeholders within selected Nigerian healthcare facilities. Rather than making claims about the entire Nigerian healthcare sector, the study provides empirical facility-level evidence from four selected healthcare institutions, drawing on responses from patients and staff categories involved in handling or being affected by personal health data processing. By examining awareness, institutional practices, compliance challenges, and perceptions of governance controls, the study contributes to bridging the gap between normative legal expectations and real-world practices that remains underexplored in the Nigerian healthcare context (Idoko et al., 2024; Imoisi & Ottah, 2025).

2. LITERATURE REVIEW

The intersection of data protection and privacy has received growing scholarly attention, particularly in sectors that process highly sensitive personal information such as healthcare. Privacy is often treated both as an individual right and as a social value that supports trust and orderly participation in modern institutions (Pecorino, n.d.). This dual framing shapes how laws, policies, and ethical practices are developed in relation to data governance. In healthcare, privacy is not merely a technical or legal requirement; it is directly tied to autonomy, trust in care relationships, and the fair handling of health information in clinical and administrative contexts (Solove, 2009; Knijnenburg et al., 2022; Conduah, Ofoe, & Siaw-Marfo, 2025). As health systems adopt digital records and networked platforms, the need for enforceable governance arrangements becomes more urgent, because the consequences of misuse, disclosure, or breach of health information can be severe for both patients and institutions.

2.1 Conceptual Foundations of Privacy

Scholars have long debated the foundations of privacy and its relevance to institutional handling of personal information. Johnson (1993) positions privacy as a core element of individual autonomy, arguing that control over personal information is central to ethical personhood. Moor (1997) extends this discussion by introducing the idea of "zones of privacy," proposing that privacy is context-sensitive and must be balanced against competing societal interests such as security and public welfare. Altman's work, discussed in contemporary privacy scholarship, similarly conceptualizes privacy as "selective control of access to self," which aligns with the need for boundary-setting in professional interactions, including those occurring in healthcare environments (Knijnenburg et al., 2022). These conceptualizations matter for healthcare because patients disclose information in contexts where vulnerability is high, and institutional actors clinicians, administrative staff, and technical personnel must manage that information in ways that protect confidentiality while enabling care delivery. Sociological and contextual approaches reinforce the view that privacy expectations are shaped by social roles and norms rather than being identical across all settings. Nissenbaum's theory of contextual integrity, for instance, argues that the appropriateness of collecting and sharing personal data depends on context, purpose, and established informational norms, meaning that privacy violations can occur even when data sharing is technically permitted but socially inappropriate (Knijnenburg et al., 2022). In healthcare, this insight is particularly relevant because the legitimacy of data flows depends not only on technical access controls but also on whether disclosures align with patient expectations, professional ethics, and institutional purpose.

From a legal standpoint, a recurring challenge in privacy enforcement is ensuring consistent interpretation of what constitutes personal data and how obligations apply across different institutional settings. In Nigeria, this challenge is addressed within the contemporary framework established by the Nigeria Data Protection Act (NDPA) 2023 and reinforced through the General Application and Implementation Directive (GAID) 2025. The Directive emphasizes that data controllers and processors must assess the "material context" of personal data processing in line with constitutional rights and statutory objectives (Nigeria Data Protection Commission, 2025, Article 2). It further clarifies that where data protection provisions conflict, the NDPA takes precedence, supporting harmonization of privacy enforcement nationwide (Nigeria Data Protection Commission, 2025, Article 3). These provisions are important for healthcare because they provide a basis for consistent interpretation and application of privacy obligations in a sector where sensitivity and risk exposure are inherently high.

2.2 Privacy and Trust in Health Data Governance

Trust is a central theme in privacy discussions, especially in data-driven environments like healthcare where effective service delivery depends on patient willingness to disclose accurate and complete information. Waldman (2018) argues that privacy protection functions as a trust-supporting mechanism by shaping expectations about how institutions will behave. In technical governance research, Mbanaso et al. (2012) propose trust negotiation approaches in which access to information is conditional upon mutual trust and agreed criteria, shifting emphasis away from purely rigid access controls toward relational governance. However, trust-based mechanisms are not widely implemented due to institutional inertia, technical complexity, and cost constraints, which often lead institutions to rely on baseline controls that may be insufficient for complex modern data ecosystems (Mbanaso et al., 2012).In Nigeria, privacy is constitutionally protected under Section 37 of the 1999 Constitution, providing a foundational basis for protecting personal communications that may include health information. Sector-relevant instruments such as the National Health Act (2014) further support confidentiality expectations in health settings, while the earlier NDPR framework also articulated general obligations for lawful and secure handling of personal data (Federal Government of Nigeria, 2014; NITDA, 2019). Nonetheless, Conduah et al. (2025) observe that across African contexts, privacy regimes often face practical obstacles such as weak enforcement authority, limited stakeholder engagement, and interoperability challenges between health systems, all of which can undermine implementation in clinical environments.

Empirical studies suggest that these challenges are pronounced in Nigeria. Idoko, Alakwe, Ugwu, and Idoko (2024) report widespread non-compliance with NDPR provisions in hospital environments, frequently linked to inadequate infrastructure and low awareness among healthcare workers. Aloamaka (2023) similarly attributes weak data protection outcomes to lax enforcement mechanisms and fragmented oversight structures. Imoisi and Ottah (2025) reinforce these findings by emphasizing disjointed oversight and limited institutional accountability as recurring problems affecting patient data security. Taken together, this literature implies that compliance is shaped not only by the presence of legal frameworks but by whether institutions operationalize privacy through visible governance structures, staff capacity development, monitoring routines, incident readiness, and practical safeguards aligned with real workflows.

2.3 Gaps in Literature and Link to the Present Study

Although theoretical explorations of data privacy are extensive, context-specific empirical evidence from low- and middle-income settings remains limited, particularly studies that link regulatory expectations to measurable institutional practices in healthcare. The NDPA (2023) and GAID (2025) implicitly recognize implementation constraints by emphasizing practical measures such as internal sensitization, routine audit expectations, and lawful bases for processing, which are intended to translate privacy principles into day-to-day practice (Nigeria Data Protection Commission, 2025, Articles 7, 15–17). Without systematic implementation strategies and routine staff training at institutional level, legal frameworks may remain largely formal rather than operational.

This study contributes to addressing the identified gap by empirically evaluating data protection practices and compliance-related perceptions within selected Nigerian healthcare facilities. By examining awareness of data protection regulation, perceived institutional safeguards, governance policy visibility, monitoring practices, training, incident response awareness, consent clarity, and perceived barriers, the study provides facility-level evidence on how privacy governance requirements translate into action or inaction in practice. In doing so, it supports calls in the literature for more empirical work that connects national policy aspirations to institutional realities and strengthens trust in healthcare data governance structures (Idoko et al., 2024; Imoisi & Ottah, 2025).

3. METHODOLOGY

3.1 Research Design

This study employed a cross-sectional quantitative survey design to examine data protection and privacy compliance practices within selected healthcare facilities in Nigeria. A cross-sectional approach was considered suitable because the aim was to capture, at a single point in time, how different stakeholder groups within healthcare settings understand data protection obligations and how they perceive the existence and functioning of compliance controls such as training, monitoring, policies, consent procedures, and breach preparedness. The study relies on structured questionnaire data and therefore uses descriptive statistics to summarize response patterns, while Spearman's rank correlation is used as an exploratory test of association for selected ordinal variables measured on Likert-type scales. The analytical strategy is aligned with the instrument structure and the level of measurement of the variables, and it does not presume causal relationships because the design does not support causal inference.

3.2 Study Setting, Units of Analysis, and Scope of Inference

The study was conducted across four healthcare facilities in Nigeria. These facilities represent practical environments in which sensitive personal and health-related data are routinely processed for clinical care, administrative coordination, record management, and digital service delivery. The unit of analysis is the individual respondent, and results are interpreted as perceptions and self-reports from respondents within the participating facilities. Because the study was facility-based and the effective sample was modest, the scope of inference is intentionally restricted to the surveyed facilities and respondents; conclusions are therefore framed as evidence from selected sites rather than claims about the entire Nigerian healthcare sector.

3.3 Population, Eligibility, and Participant Categories

The study population comprised stakeholders who either process health data as part of their institutional roles or are directly affected by such processing as data subjects. Respondents were drawn from four main categories: patients receiving care within the facilities, clinicians involved in clinical documentation and use of patient information, management staff involved in oversight and administrative decision-making, and IT/system administrators responsible for the technical systems through which health data are stored, accessed, transmitted, or secured. Inclusion in the study required that the respondent belonged to one of these categories within the selected facilities during the study period and voluntarily agreed to participate. Responses were screened for completeness at the point of data preparation, and only questionnaires that contained sufficient valid responses for analysis were retained in the final dataset.

3.4 Sampling Approach, Recruitment, and Achieved Sample

A total of 100 questionnaires were distributed across the four facilities. Recruitment was organized to reach all stakeholder categories, reflecting the study's emphasis on comparing awareness and perceived practices across groups that interact with patient data in different ways. Although distribution was broad, the achieved valid response count was 38, yielding an effective response rate of 38%. The analyzed dataset comprised 38 respondents made up of 19 patients, 8 clinicians, 6 IT/system administrators, and 5 management staff. This achieved sample is treated as an empirical snapshot of practices and perceptions in the selected facilities rather than a statistically representative sample of Nigerian healthcare institutions. The modest response rate and the possibility that respondents who participated may differ systematically from those who did not are recognized as potential sources of non-response bias. For that reason, the study avoids overgeneralization and focuses on careful, facility-bounded interpretations.

3.5 Regulatory Benchmark and Operational Compliance Framework

Assessment of compliance was anchored in Nigeria's current data protection regime. The study is framed primarily by the Nigeria Data Protection Act (NDPA, 2023) and the Nigeria Data Protection Commission's General Application and Implementation Directive (GAID, 2025), which together provide the statutory and implementation expectations for data controllers and processors. References to the Nigeria Data Protection Regulation (NDPR, 2019) are treated as contextual and transitional, reflecting its historical role and continued mention in organizational practice where legacy compliance language persists. To translate regulatory expectations into measurable survey constructs, the questionnaire was structured around operational domains that reflect practical compliance activities in healthcare data environments. These domains capture awareness of obligations, reported safeguards for storage and transfer, policy and governance environment, monitoring and accountability practices, staff training and sensitization, incident response readiness for breach events, consent and transparency practices, and perceptions of barriers such as resource constraints and third-party risk exposure. Throughout the manuscript, results are mapped back to these domains to ensure that compliance claims are explicitly tied to defined constructs rather than broad or undefined notions of "compliance."

3.6 Data Collection Instrument and Measurement Structure

Data were collected using a structured questionnaire composed primarily of closed-ended questions. Items were designed to elicit respondent perceptions and experiences regarding the presence, frequency, or adequacy of compliance practices. Likert-type response formats were used where ordinal measurement was appropriate, including agreement scales for training and consent perceptions and awareness scales for incident response readiness. The instrument also included categorical items to capture respondent characteristics and role categories, as well as multi-select items to capture perceived barriers to compliance, recognizing that compliance challenges in real settings are often multi-factorial. In the revised manuscript, the final questionnaire length should be stated consistently, and the domains should be clearly described with representative item examples. Where any composite scores are created from multiple items, the scoring logic should be explicitly described so that a reader can reproduce the measures and interpret the meaning of high or low scores.

3.7 Validity and Reliability Procedures

To support content validity, the instrument was developed to reflect concrete compliance expectations and widely recognized data protection governance elements applicable to healthcare processing, including training, monitoring, safeguards, and breach preparedness. Items were worded to be understandable to both staff and patients, while still capturing concepts that correspond to compliance practices and institutional accountability. Where expert review or pilot testing was conducted, this process should be described transparently, including who reviewed the instrument, what changes were made, and how ambiguous items were improved. Reliability assessment depends on whether the instrument includes multi-item scales that measure the same construct. Where multi-item domain scales exist, internal consistency may be estimated using Cronbach's alpha and reported by domain, interpreted cautiously in light of the modest effective sample size. Where constructs are measured by single items, reliability cannot be meaningfully estimated through internal consistency metrics; in such cases, the study treats responses as standalone indicators and reports them descriptively. This approach preserves methodological honesty and prevents overstating measurement precision.

3.8 Data Collection Procedure and Ethical Safeguards

Questionnaires were administered within the participating facilities through in-person distribution during the data collection period. Respondents were informed about the purpose of the study, the voluntary nature of participation, and the confidentiality of their responses. No personally identifying information was required for participation, and responses were handled in a manner intended to protect privacy and minimize risk. Completed questionnaires were compiled for analysis and screened for completeness. The final dataset retained only responses deemed sufficiently complete to support analysis. Aggregated reporting was used throughout to avoid identifying individuals or linking sensitive perceptions to specific persons.

3.9 Data Preparation, Missing Data, and Denominator Rules

Because the questionnaire included items that were not equally applicable to every respondent group and because item-level non-response occurred, denominators vary across analyses. For example, questions related to incident response planning were applicable primarily to staff categories, while some governance or monitoring questions were answered only by respondents who indicated familiarity with policy structures. Rather than forcing a single denominator across the entire results section, the study applies an item-valid approach in which each table or figure reports the exact number of valid responses used for that analysis. This decision is methodological as well as editorial: it ensures that percentages are interpretable, allows the reader to see where missingness is concentrated, and prevents misleading comparisons that would occur if absent responses were silently treated as negative or neutral. In the revised manuscript, every table and figure must therefore state the relevant respondent subgroup and the denominator used so that results remain transparent and reproducible.

3.10 Statistical Analysis and Interpretation Rules

Analysis proceeded in two stages. First, descriptive statistics were computed to summarize the distribution of responses across awareness levels, reported safeguards, governance policy availability, training and sensitization frequency, perceptions of consent clarity, and perceived barriers to compliance. Frequencies and percentages were used because many variables are categorical or ordinal, and the study's objective is primarily evaluative and descriptive rather than predictive. Second, exploratory association analysis was conducted using Spearman's rank correlation for selected ordinal variables related to monitoring, awareness activities, and adherence indicators. Spearman's rho was chosen because it does not require normally distributed variables and is appropriate for ranked or ordinal data. Correlation outputs are interpreted strictly as associations, not evidence that one factor causes another, particularly given the cross-sectional design and the small complete-case subgroup size for the correlation analysis. Where correlation tables are presented, the revised manuscript should report the sample size used for each correlation set and, where applicable, include significance testing information and clear definitions of how each correlated variable was constructed.

Techniques for Data Analysis and Model Specification

This research used thematic analysis techniques.

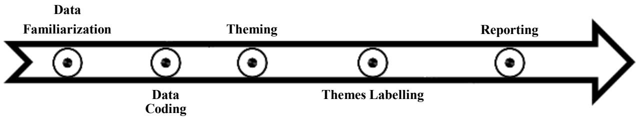


Figure 1: Thematic Analysis Process Used in the Study

As shown in figure 1, the systematic model includes several steps:

Data Familiarization: Collected data was thoroughly reviewed to get familiar with it.

Data Coding: Related data was extracted from the survey responses and separated using codes to depict the content.

Theming: Codes with similar patterns were combined to form themes or discarded if too vague. Generated codes were compared with the data set to ensure accurate representations of the data.

Themes Labelling: The themes were clearly defined and named, representing the patterns they capture.

Reporting: The research documented the themes and corresponding data extracts supporting each theme and provided explanations of each theme's significance within this research context.

4. DATA ANALYSIS AND RESULTS

A total of thirty-eight (38) valid questionnaires were included in the analysis. The respondent composition was nineteen (19) patients, eight (8) clinicians, six (6) IT/system administrators, and five (5) management staff. Because some questions were directed only at particular categories (for example, incident response planning questions directed to workers), and because some respondents skipped certain items, the denominator varies across analyses. In all tables and figures, the specific denominator used for each result is stated explicitly. Percentages are therefore calculated using the number of valid responses to that specific item (item-valid responses), rather than the full sample in every case.

4.1 Awareness of Data Protection Regulation

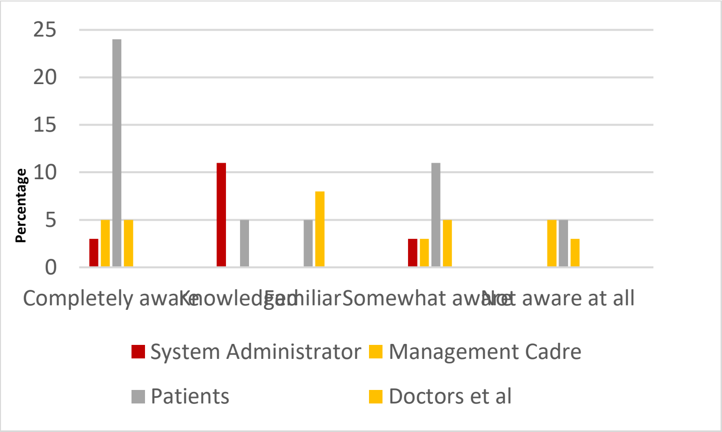
Respondents' awareness of the Nigeria Data Protection Regulation (NDPR) was assessed across the full sample (n=38). Table 1 summarizes the distribution of awareness levels. Fourteen respondents (37%) reported being completely aware of the NDPR, while eight (21%) indicated they were only somewhat aware, meaning they knew of its existence but not its details. Six respondents (16%) described themselves as knowledgeable but not completely aware, five (13%) reported being familiar with some details, and five (13%) reported that they were not aware at all.

Table 1: Respondents' Level of Awareness of the Nigeria Data Protection Regulation (NDPR)

	Frequency	**Percentage**
Completely aware	14	37
Knowledged (well-aware but not completely)	6	16
Familiar (aware of some details)	5	13
Somewhat aware (aware of its existence but not the details)	8	21
Not aware at all	5	13
Total	38	100

To clarify how awareness varied by stakeholder category, Figure 2 presents awareness distribution within each respondent group. Within the patient group (n=19), a relatively larger share reported complete awareness compared to staff groups. In contrast, the IT/system administrator group (n=6) showed lower reported complete awareness relative to patients, while clinicians (n=8) and management staff (n=5) demonstrated mixed levels of awareness across the intermediate categories. Because these subgroup sizes are small, the figure is interpreted as a descriptive pattern within the participating facilities rather than a sector-wide estimate.

Figure 2: Awareness of Nigeria Data Protection Regulation (NDPR) by Respondent Category



4.2 Measures Reported for Protecting Personal Data in Storage and Transfer

Respondents were asked to indicate measures used to protect personal data during storage and transfer. Table 2 reports valid responses for this item using the denominator shown in the table. The most frequently reported measure was the presence of a secure network (29%). Encryption and legal/compliance checks were also commonly reported (21% each). Access controls were reported by 14% of respondents. Smaller proportions reported regular backups, physical security, and secure email/file sharing (7% each), while a similar proportion indicated that they did not know what measures were used (7%). No respondents selected data retention policies, secure disposal, audit trails/logging, or vendor/third-party security practices. These non-selections are reported as “not identified by respondents” and should not be interpreted as proof that such controls are absent in practice; rather, they reflect what respondents reported within this dataset.

Table 2: Measures Reported to Protect Personal Data During Storage and Transfer

	Frequency	**Percentage**
Encryption	3	21
Access Controls	2	14
Regular Backups	1	7
Physical Security	1	7
Data Retention Policies	0	0
Secure Disposal	0	0
Secure Network	4	29
Secure Email and File Sharing	1	7
Audit Trails and Logging	0	0
Vendor and Third-Party Security	0	0
Legal and Compliance Checks	3	21

Others – Don't Know	1	7

4.3 Breach Preparedness: Awareness of Incident Response Plans

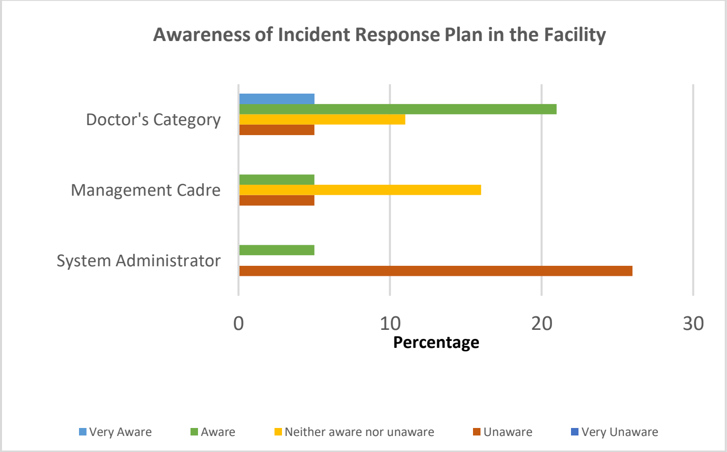
Awareness of incident response plans for breach events was assessed among healthcare workers only (clinicians, IT/system administrators, and management staff), yielding a staff-only denominator of nineteen (n=19). Table 3 shows that seven respondents (37%) reported being unaware of any incident response plan in their facility. Six respondents (32%) reported being aware, five (26%) selected a neutral position (neither aware nor unaware), and one respondent (5%) reported being very aware. No respondents selected "very unaware." The overall pattern suggests that incident response planning is not consistently visible or communicated among staff in the participating facilities.

Table 3: Healthcare Workers' Awareness of Incident Response Plans for Data Breach Events

	Frequency	**Percentage**
Very Unaware	0	0
Unaware	7	37
Neither aware nor unaware	5	26
Aware	6	32
Very Aware	1	5
Total	19	100

Figure 3 presents the same item by worker category to show how perceptions differ across clinicians, management staff, and IT/system administrators. The distribution indicates that a notable proportion of IT/system administrators reported being unaware, while clinicians and management staff were more dispersed across neutral and aware response categories. Because subgroup denominators are small (clinicians n=8; IT/system administrators n=6; management staff n=5), these patterns are interpreted descriptively for the participating facilities and not as population-level differences.

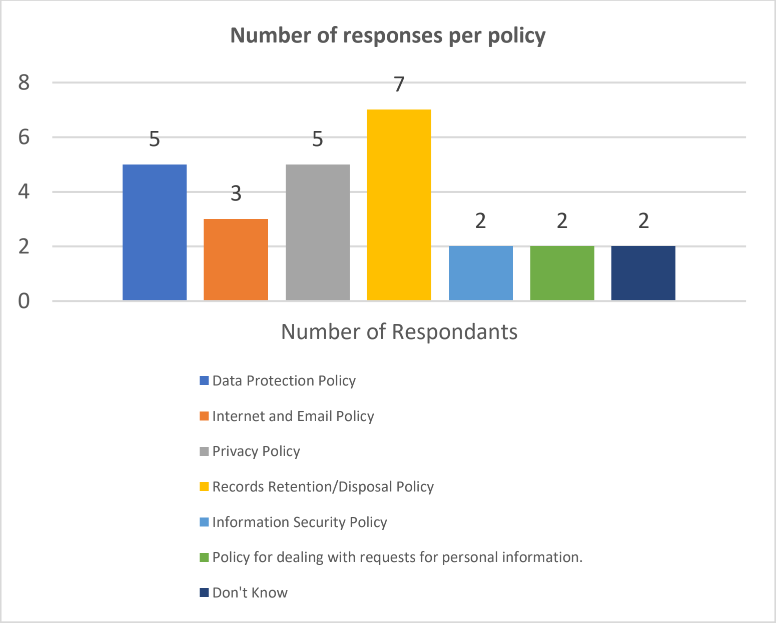
Figure 3: Awareness of Incident Response Plans by Respondent Category



4.4 Data Governance Policies and Monitoring Practices

Respondents were asked to identify which data governance policies they believed were present within the clinic environment. Figure 4 summarizes the policies most frequently acknowledged. Records retention/disposal was the most acknowledged policy, selected by seven respondents. Data protection policy and privacy policy were each selected by five respondents, while internet and email policy was acknowledged by three respondents. Only two respondents acknowledged the presence of an information security policy or a policy for personal information, and two respondents indicated that they did not know which policies existed. The pattern suggests uneven awareness of governance documentation and varying visibility of formal policy structures.

Figure 4: Availability of Data Governance Policies in the Clinic



Monitoring of adherence to clinic policies was measured using a frequency item that received eleven valid responses (n=11). Table 4 shows that five respondents (45%) reported that adherence is often monitored. Two respondents (18.2%) reported monitoring occurs always, and two respondents (18.2%) reported it occurs sometimes. One respondent (9.1%) selected rarely, and one respondent (9.1%) provided no response within the item's response structure as captured in the dataset. No respondent selected "never." These results indicate that monitoring is perceived to occur with some regularity among those who responded, but the limited denominator requires cautious interpretation

Table 4: Frequency of Monitoring Adherence to Clinic Policies

	Frequency	**Percentage**
Never	0	0
Rarely	1	9.1
Sometimes	2	18.2
Often	5	45
Always	2	18.2
No Response	1	9.1
Total	11	100

The frequency with which data security and privacy awareness activities are raised in facilities was answered by eighteen respondents (n=18). Table 5 shows that seven respondents (39%) reported awareness activities are always raised, while four respondents (22%) indicated they occur often and another four (22%) indicated they occur sometimes. Two respondents (11%) indicated such awareness is rarely raised, and one respondent (6%) reported it is never raised. These results suggest that awareness activities exist within the participating facilities but may vary in regularity.

Table 5: Frequency of Data Security and Privacy Awareness in Healthcare Facilities

	Frequency	**Percentage**
Never	1	6
Rarely	2	11
Sometimes	4	22
Often	4	22
Always	7	39
No Response	0	0
Total	18	100

Perceptions of external compliance monitoring by the GAID were captured using an item with eleven valid responses (n=11). As shown in Table 6, four respondents (36.3%) reported that GAID monitoring visits sometimes occur, while three respondents (27.2%) reported visits rarely occur. Two respondents (18.2%) indicated visits always occur, and one respondent (9.1%) reported visits often occur. One respondent (9.1%) provided no response in the dataset. These results should be interpreted as respondent perceptions rather than administrative records of regulatory visits.

Table 6: Frequency of NDPA Monitoring Visits to Healthcare Facilities

	Frequency	**Percentage**
Never	0	0
Rarely	3	27.2
Sometimes	4	36.3
Often	1	9.1
Always	2	18.2
No Response	1	9.1
Total	11	100

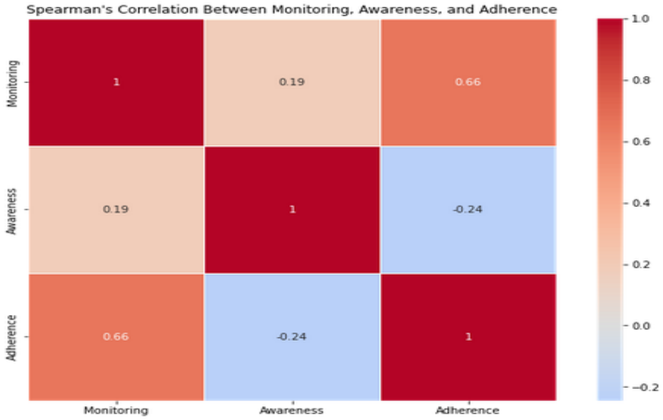
4.5 Exploratory Associations Between Monitoring, Awareness Activities, and Adherence

To explore whether monitoring practices and awareness activities are associated with reported adherence, an exploratory analysis was conducted using Spearman's rank correlation. Only respondents with complete responses across the variables used in this analysis were included, resulting in a complete-case subgroup of eleven (n=11). Table 7 presents the correlation matrix. Monitoring and adherence showed a positive association (rho = 0.656). Awareness activities and adherence showed a weak negative association (rho = −0.244). These findings are interpreted as associations within the complete-case subgroup and do not imply causation, especially given the cross-sectional design and the small denominator.

Table 7: Spearman's Correlation Matrix Between Monitoring, Awareness, and Adherence

	Monitoring	**Awareness**	**Adherence**
Monitoring	1.000000	0.187194	0.656371
Awareness	0.187194	1.000000	-0.244033
Adherence	0.656371	-0.244033	1.000000

Figure 5: Spearman's Correlation Matrix Between Monitoring, Awareness, and Adherence



4.6 Perceived Barriers to Compliance

Perceived factors contributing to non-compliance were collected using a multi-select item. Seventeen respondents provided valid answers to this question (n=17), and because multiple selections were allowed, percentages do not sum to 100%. Table 8 shows that lack of awareness was the most frequently selected factor (71%), followed by insufficient resources (53%) and rapid technological changes (47%). Third-party risks were also frequently selected (41.1%), while poor data governance practices were selected by 24% of respondents. Complexity of regulations, cultural and organizational factors, and low enforcement risk or penalties were each selected by 18% of respondents. These results describe perceived barriers reported by respondents and should be interpreted as perceived contributors rather than verified causal determinants.

Table 8: Perceived Factors Contributing to Non-Compliance with Data Protection and Privacy in Hospitals

	Frequency	**Percentage**
Lack of Awareness	12	71
Insufficient Resources	9	53
Poor Data Governance Practices	4	24
Rapid Technological Changes	8	47
Third-Party Risks	7	41.1
Complexity of Regulations	3	18
Cultural and Organizational Factors	3	18
Low Enforcement Risk or Penalties	3	18

As shown in Table 9, 39% of respondents *agreed* that employees receive training on data protection and relevant laws, while 28% *strongly disagreed*. Meanwhile, 11% each either *disagreed*, *strongly agreed*, or remained *neutral* (*neither disagree nor agree*), suggesting mixed perceptions about the consistency and availability of staff training on data governance.

Table 9: Respondents' Agreement on Whether Employees Receive Training on Data Protection Laws

	Frequency	**Percentage**
Strongly Disagree	5	28
Disagree	2	11
Neither disagree nor agree	2	11
Agree	7	39
Strongly Agree	2	11
Total	18	100

As shown in Table 10, many respondents (68%) *agreed* that their hospital's method of collecting patient consent is clear and well-informed, while 21% *strongly agreed*. Only 11% remained *neutral*, suggesting overall confidence in consent procedures among participants.

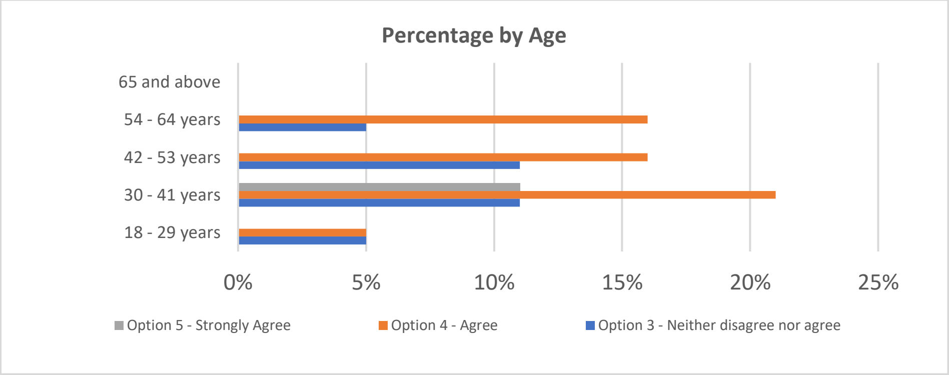
Table 10: Respondents' Agreement on the Clarity and Quality of Patient Consent Collection

	Frequency	**Percentage**
Neither disagree nor agree	2	11
Agree	13	68
Strongly Agree	4	21
Total	19	100

As illustrated in **Figure 6**, 16% of respondents aged 54–64 *agreed* that the hospital's consent process is clear, while 5% were *neutral*. Among those aged 42–53, 16% also *agreed* and 11% were *neutral*. For participants aged 30–41, 21% *agreed*, and 11% each *strongly agreed* or gave *neutral* responses.

Lastly, among 18–29-year-olds, 5% *agreed* and 5% were *neutral*. These findings suggest that perceptions of consent clarity were generally positive across age groups, though younger respondents showed slightly lower agreement levels.

Figure 6: Perceptions of Patient Consent Clarity by Age Group



Taken together, the findings indicate that awareness of data protection regulation exists within the participating facilities but is not uniform across respondent categories. Reported security and governance controls emphasize network protection and encryption, while several important control areas such as audit trails/logging, secure disposal, data retention policies, and third-party security governance were not identified by respondents in this dataset. Staff responses also indicate that incident response planning is not consistently visible across worker categories. Perceived compliance barriers are dominated by awareness and resource constraints, with technological change and third-party risks also commonly reported. Exploratory association analysis conducted on complete cases suggests that monitoring is positively associated with adherence, while awareness activities show a weak negative association with adherence; however, these associations should be interpreted cautiously due to the small complete-case sample and the cross-sectional design. Overall, the results point to the importance of moving from general awareness to operational compliance mechanisms, including routine training, clearer internal monitoring structures, and formal breach preparedness procedures, within the context of facility-level governance and accountability.

5. CONCLUSION

This study assessed data protection and privacy compliance practices in four selected healthcare facilities in Nigeria using a cross-sectional survey of 38 valid respondents. The findings indicate that awareness of data protection regulation exists but varies across stakeholder groups and does not consistently translate into uniformly reported compliance practices. Reported safeguards focused mainly on secure networks and encryption, while several important governance and accountability controls (such as audit trails/logging, secure disposal, and vendor/third-party security practices) were not identified by respondents. Among healthcare workers, awareness of breach incident response plans was also inconsistent, suggesting gaps in preparedness and internal communication.

Perceived barriers to compliance were dominated by lack of awareness, resource constraints, rapid technological change, and third-party risks, while perceptions of staff training were mixed. Exploratory correlation results suggest monitoring is associated with higher reported adherence, but these associations should be interpreted cautiously given the small complete-case sample and the cross-sectional design. Overall, the results support the need for stronger facility-level monitoring, routine role-specific training, clearer breach response procedures, and improved governance of third-party risks, with conclusions limited to the participating facilities rather than the Nigerian healthcare sector as a whole.

ACKNOWLEDGMENT

I am immensely grateful to my husband and children for their unending support, Prof. Uche M. Mbanaso, Dr. T.K Anyachebelu, Dr. S. E. Chaku, Mr. Salihu Muhammad Bashir, and every staff of Department of Centre for Cyberspace Studies, who contributed to the success of this paper.

REFERENCES

Aloamaka, P. (2023). *Data protection and privacy challenges in Nigeria: Lessons from other jurisdictions*. UCC Law Journal, *3*(1), 281–321. https://doi.org/10.47963/ucclj.v3i1.1259

Altman, I. (1975). The environment and social behavior: Privacy, personal space, territory, crowding. Brooks/Cole

Conduah, A. K., Ofoe, S., & Siaw-Marfo, D. (2025). Data privacy in healthcare: Global challenges and solutions. Digital Health, 11, 1–19. https://doi.org/10.1177/20552076251343959

European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Federal Government of Nigeria. (2014). *National Health Act, 2014* (Act No. 8 of 2014). Federal Ministry of Health. https://scorecard.prb.org/wp-content/uploads/2019/06/Nigeria-National-Health-Act-2014.pdf

Idoko, B., Alakwe, J. A., Ugwu, O. J., & Idoko, J. E. (2024). Enhancing healthcare data privacy and security: A comparative study of regulations and best practices in the US and Nigeria. Magna Scientia Advanced Research and Reviews, 11(2), 151–167. https://doi.org/10.30574/msarr.2024.11.2.0110

Johnson, D. G. (1994). Computer ethics (2nd ed.). Prentice Hall.

Keshta, I., & Odeh, A. (2020). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(6), Article 100560. https://doi.org/10.1016/j.eij.2020.07.003

Knijnenburg, B. P., Xu, H., Wisniewski, P., Lipford, H. R., Proferes, N., & Romano, J. (2022). Privacy theories and frameworks. In Modern socio-technical perspectives on privacy (pp. 21–46). Springer. https://doi.org/10.1007/978-3-030-82786-1_2

Mathews, A. W. (2015, February 24). Anthem: Hacked database included 78.8 million people. The Wall Street Journal. https://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364

Mbanaso, U., Cooper, G., & Djemame, K. (2012). Privacy-aware trust-based access control infrastructure using XACML. International Journal of Trust Management in Computing and Communications, 1(1), 89–104. https://salford-repository.worktribe.com/output/1433671/privacy-trust-access-control-infrastructure-using-xacml

Moor, J. H. (1997). Towards a theory of privacy in the information age. ACM SIGCAS Computers and Society, 27(3), 27–32. https://doi.org/10.1145/270858.270866

National Information Technology Development Agency (NITDA). (2019). Nigeria Data Protection Regulation (NDPR). https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf

Nigeria Data Protection Act. (2023). Nigeria Data Protection Act, 2023. Federal Republic of Nigeria. https://ndpc.gov.ng/wp-content/uploads/2023/06/NIGERIA-DATA-PROTECTION-ACT-2023.pdf

Nigeria Data Protection Commission. (2025, March 20). General Application and Implementation Directive (GAID) 2025. https://ndpc.gov.ng/wp-content/uploads/2025/03/NDP-ACT-GAID-2025-MARCH-20TH.pdf

Nigerian Communications Commission. (2023). 2023 year-end performance report [PDF]. https://www.ncc.gov.ng/sites/default/files/2025-04/2023-YEAR-END-PERFORMANCE-REPORT.pdf

Office for Civil Rights. (2018, October 15). Anthem pays OCR $16 million in record HIPAA settlement following largest health data breach in history. U.S. Department of Health & Human Services. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/anthem/index.html

Pecorino, P. A. (n.d.). Introduction to philosophy. Queensborough Community College, The City University of New York. https://www.qcc.cuny.edu/socialSciences/ppecorino/INTRO_TEXT/CONTENTS.htm

Solove, D. J. (2009). Understanding privacy (eBook ed.). Harvard University Press. https://www.hup.harvard.edu/books/9780674043855

The HIPAA Journal. (2021, December 30). Largest healthcare data breaches of 2021. https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2021/

Regan, P. M. (1995). Legislating privacy: Technology, social values, and public policy. University of North Carolina Press

U.S. Congress. (1996). Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936. https://www.congress.gov/bill/104th-congress/house-bill/3103CCP

Waldman, A. E. (2018). What does trust mean for privacy? In Privacy as trust: A new framework for data protection (pp. 39–68). Cambridge University Press. https://www.cambridge.org/core/books/abs/privacy-as-trust/what-does-trust-mean-for-privacy/0EB2D35DDBD6481EAB58F588555FD6B5