HEALTH DATA GOVERNANCE AND THE RIGHT TO HEALTH DATA PROTECTION IN NIGERIA: FRAGMENTATION, PROPORTIONALITY AND REGULATORY GAPS

Oghomwen Rita Ohiro [*] **& Oghosa Annabel Igbinedion** [**]

Abstract

The rapid digitisation of healthcare systems and the growing reliance on advanced data analytics have intensified concerns regarding the lawful processing, secondary use, and protection of sensitive health data. Although the Nigeria Data Protection Act (NDPA) represents a major legislative development and reflects a risk-sensitive framework for the protection of personal data. The question is whether the existing regulatory architecture sufficiently safeguards health data within an increasingly complex digital ecosystem. This paper aims to assess the framework of health data governance in Nigeria critically. It examines how the NDPA, together with the General Application and Implementation Directive (GAID) 2025, and other sectoral instruments, are able to address fragmentation, proportionality, anonymisation, and exemptions in the processing of health data. It uses a doctrinal research approach to assess the proportionality requirements under the NDPA framework. It also conducts a comparative analysis of South Africa's Protection of Personal Information Act (POPIA) and the General Data Protection Regulation of the European Union to provide insight into the design choices of regulations. Although the NDPA provides a robust and rights-based foundation for the protection of health data, it is not detailed in terms of proportionality architecture, prior authorisation for high-risk processing, and anonymisation standards. The GAID 2025 aims to solve the issue of fragmentation in a way by providing interpretative guidance, but it does not solve the structural disjunctions that exist in the health data governance system as a whole. The result is a system that is normatively robust but operationally patchy in terms of protecting sensitive health data. The paper reframes the issue of health data governance not only as a matter of compliance but as a structural human rights issue. The paper argues that the issue of health data protection cannot be addressed without proportionality safeguards, research limitations, and regulatory coordination.

Keywords: Health Data Governance, Nigeria Data Protection Act, Proportionality, Fragmentation, Human.

[*] LLB, BL, LLM, PhD, Email: oghomwen.igbinedion@uniben.edu Phone: 07062368221, Senior Lecturer, Department of Public Law, Faculty of Law, University of Benin, Benin City.

[**] LLB, BL, LLM, Email: oghosa.igbinedion@uniben.edu Phone: 08174792968, Lecturer, Department of Jurisprudence and International Law, Faculty of Law, University of Benin, Benin City.

1. Introduction

The integration of sophisticated analytical tools into the healthcare delivery system has completely transformed the way medical information is created, processed, and analysed.[1] Contemporary health systems now operate within interconnected digital infrastructures that draw upon multiple streams of information, which include electronic health records, medical imaging systems, and clinical decision support systems.[2] The increasing digitisation of healthcare systems has therefore transformed the collection, processing, and use of health data, positioning data as a central component of modern healthcare delivery. [3] The implementation of these frameworks is a fundamental change from traditional healthcare concepts from conventional models like delivery models to more data-driven and personalized models.[4] Evidence from healthcare organisations suggests that the deployment of advanced analytical frameworks has strengthened operational performance and improved clinical results, largely by enabling more strategic resource deployment and more efficient regulation of patient traffic.[5]

In Nigeria, this transformation reflects a broader global shift towards digitally enabled healthcare, marked by the expansion of electronic health records, telemedicine services, and data-driven public health.[6] The ability to integrate monitoring and evaluation data with geo-spatial mapping technologies enables the authorities to develop models of ―patient traffic‖ and thereby deploy the scarce resource of healthcare professionals more efficiently.[7]

Patient health information obtained from electronic health records, medical images, devices, and genomic research is useful in enabling healthcare service providers to make more informed decisions.[8] Similarly, advanced statistical techniques in the field of data analytics, including AI

---

1 Jyoti Aggarwal, ‗Data Analytics in Healthcare: Revolutionizing Personalized Medicine and Diagnosis' (2025) *European Journal of Computer Science and Information Technology*,13(20), 105.

2 Ibid.

3 Angelos I Stoumpos and others, ‗Digital Transformation in Healthcare: Technology Acceptance and Its Applications' (2023) *Int J Environ Res Public Health* 20(4), <https://pmc.ncbi.nlm.nih.gov/articles/PMC9963556/> accessed 10 January 2026

4 Ibid.

5 Ibid.

6 Adaeze E Egwudo, ‗Integrating digital health technologies into the healthcare system: Challenges and opportunities in Nigeria' (2025) *PLOS Digit Health* 4(7) e0000928. doi: 10.1371/journal.pdig.0000928

7 Joel Aniebe, ‗How Nigeria's Fresh Approach to Data Collection could Uncover Key Health Insights' < https://diagnostics.roche.com/global/en/healthcare-transformers/article/data-in-healthcare-primary-system.html#:~:text=For%20Nigeria%20to%20unlock%20clinical,pharma%20industry%20and%20Academic%20community.> accessed 16 February 2026.

8 Ibid.

and machine learning algorithms, can facilitate the early detection of diseases.[9] These significantly improve the optimisation of resources, reduction of errors, and personalisation for the patient.[10]

This trend in the evolution of data collection policies is further exemplified by several policy initiatives.[11] Nigeria is currently piloting a data collection model referred to as the —hardware-first‖ approach in primary health centers.[12] This approach has seen the introduction of robust offline-enabled devices such as e-ink tablets, which enable the collection of longitudinal patient data and later synchronize the data in the cloud.[13] The aim of these innovations is the creation of a richer data set from routine patient interactions, particularly in under-resourced settings where internet connectivity is poor.[14] The objective is not only the digitisation of data but the creation of health data infrastructures that are interoperable and can be used in service planning, pharmaceutical forecasting, and even research.[15]

While these developments improve efficiency, diagnostic accuracy, and access to care, they also raise complex legal and governance challenges, particularly given the sensitive nature of health data.[16] Health data warrants heightened legal protection due to its close association with dignity, bodily integrity, and vulnerability.[17] The misuse or unauthorised processing of such data can result in stigma, discrimination, and other forms of harm. These risks are exacerbated in Nigeria by structural inequalities in healthcare provision,[18] limited institutional capacity, and fragmented regulatory oversight.

---

9 Ibid.
10 Ibid.
11 Aniebe (n 7).
12 Ibid.
13 Ibid.
14 Ibid.
15 Ibid.
16 H Mumtaz and others, _Current Challenges and Potential Solutions to the Use of Digital Health Technologies in Evidence Generation: A Narrative Review‘ (2023) *Front Digit Health* 5:1203945. doi: 10.3389/fdgth.2023.1203945. PMID: 37840685; PMCID: PMC10568450.
17 Studies provide a strong conceptual foundation linking health, vulnerability, autonomy, bodily integrity, and dignity, all of which are directly implicated in health information governance: B Sæteren and D Nåden, _Dignity: An Essential Foundation for Promoting Health and Well-Being‘ (2021) in G Haugan and M Eriksson , (eds.) *Health Promotion in Health Care – Vital Theories and Research [Internet] (*Springer; 2021) <https://www.ncbi.nlm.nih.gov/books/NBK585664/ doi: 10.1007/978-3-030-63135-2_7>
18 Nonye Benedeth Ezeaka _Addressing Healthcare Inequalities in Nigeria: A Communication Perspective on Advocacy and Policy Implications‘ (2025) *Journal of Advanced Research and Multidisciplinary Studies* 5(1), 1-11.

The move from a paper-based system to an automated electronic system introduces new logics of governance in healthcare delivery systems. For instance, features such as automatic triage based on predetermined parameters,[19] access control, and restriction of duplicate entries and real-time display of information centralize power and authority in decision-making within the parameters of technology. These systems, although enhancing efficiency and transparency, create a new dynamic in governance by moving the locus of power from healthcare workers to parameters of technology. While Nigeria is embracing digital and data-driven technologies in its health sector, its legal and regulatory framework governing health data has not evolved at the same pace. For instance, although several states have adopted digital health interventions, many have not enacted laws governing digital health data security and privacy.[20]

This has been exemplified in the empirical evidence from the COVID-19 pandemic in Nigeria.[21] A study conducted in the Nigerian Institute of Medical Research (NIMR) drive-through testing centre highlighted the data integrity issues, which included incomplete data, inaccurate contact information, and poor accountability.[22] In some instances, patients who were previously found to be infected with tuberculosis in the digital trials were not contacted because of inaccurate information.[23] This was attributed to the paper-based system, workforce limitations, and the lack of embedded quality control.[24] The pandemic accelerated centralised data collection and outbreak management systems but did not necessarily develop parallel oversight mechanisms for proportionality, retention, or secondary use.

This article argues that although Nigeria has established a formally robust framework for protecting health data, such as the Nigeria Data Protection Act (NDPA) 2023[25] and other legislation, its governance regime remains fragmented, under-integrated, and insufficiently responsive to the realities of data-driven healthcare. The broad public interest and research exceptions under the NDPA, coupled with limited regulatory elaboration and oversight

[19] Bosun Tijani, _Improving Data Integrity in Public Health: A Case Study of an Outbreak Management System in Nigeria‘ (2021) *Global Health Science and Practice* 9(Supplement 2) S226-S233, S230.

[20] Chukwuemeka Azubuike, _Assessing Digital Health Maturity in Nigeria: Evidence from a Sub-national Assessment Across Ten (10) States and Strategic Imperatives for Health Sector‘ (2025) *VeriXiv,* 2:258

[21] Tijani, (n 19) S228.

[22] Ibid, S228.

[23] Ibid, S227.

[24] Ibid, 226.

[25] Federal Republic of Nigeria Official Gazette No. 119 Lagos - 1st July, 2023 Vol. 110 Government Notice No. 82.

mechanisms, risk undermining confidentiality, proportionality, and ultimately the substantive realisation of the right to health.

Drawing on a doctrinal and comparative methodology, this article critically examines Nigeria's health data governance framework from a human rights perspective. It analyses the Nigeria Data Protection Act 2023, and some sector specific legislations, while drawing comparative insights from South Africa's Protection of Personal Information Act (POPIA) [26] and the European Union's General Data Protection Regulation.

2. Health Data as Sensitive Data

To understand why heightened governance is necessary, it is first important to clarify why health data occupies a distinct normative position within data protection law. Health data is different from other forms of data in that it transcends simple medical histories. It comprises a combination of structured data (such as electronic health records data and coded clinical terms), semi-structured data (such as XML-based HL7 messages), and unstructured data (including clinical notes, medical imaging, and genetic information).[27] It includes personal health information, medical histories, and treatment records.[28] The sensitivity of the data is due to the essential link to human dignity, integrity, and vulnerability. The distinguishing factor of health data from any other information is that misuse of the data and processing of the information without authorisation have the potentials for stigmatisation, persecution, and detriment.

Under the NDPA 2023, health data is classified as sensitive data.[29] This classification is particularly significant, because unlike ordinary personal data, sensitive personal data can only be processed under special circumstances mentioned in Section 30. This is perhaps in recognition of health data's intimate character and its potential to expose individuals to discrimination, stigma and other forms of harm if misused. Stangl and others argue in their _Health Stigma and Discrimination Framework' that health data is a primary driver of inequality. Health information

[26] Protection of Personal Information Act 4 of 2013, <https://popia.co.za/> accessed 16 February 2026.

[27] Mu-Hsing Kuo and others, _Health Big Data Analytics: Current Perspectives, Challenges and Potential Solutions January' (2014) *International Journal of Big Data Intelligence* 1(1/2):116.

[28] Ogbemudia Isaac Ottah, and Ekojema Imoisi, _An Appraisal of the Legal Framework for Data Security Protection for Health Institutions in Nigeria' (2025) *Journal of Current Research and Review,* 16(2) 1-11,2.

[29] Nigeria Data Protection Act, 2023, Federal Republic of Nigeria, Official Gazette No. 119 Lagos - 1st July, 2023 Vol. 110 Government Notice No. 82 (NDPA 2023), s 65.

can be used to _mark‘ individuals as different; its unauthorised disclosure triggers a process of social devaluation, leading to discrimination in employment and housing as well as an internalized stigma that undermines a patient‘s dignity. [30]

Research shows that medical records are not neutral repositories but can be active _technologies of stigma.‘[31] These healthcare record systems are capable of allowing certain behaviours by healthcare workers.[32] It has been argued that modern electronic management systems often reduce complex human lives to rigid diagnostic categories.[33] This is termed: datafication, it forces a patient into a static healthcare subject stripping away their ability to evolve or change in the eyes of the healthcare system.[34] Clinical notes act as a communication system where stigma is transferred between practitioners, in the sense that a biased noted written by one physician frames how a subsequent healthcare worker sees a patient, effectively institutionalizing a _spoiled identity.‘[35] Effective health data governance becomes imperative to prevent this socially embedded stigma from converting to institutionalized discrimination. The classification of health data as _sensitive personal data‘ under the NDPA 2023 is not merely a privacy safeguard, but a structural response to the link between health status, stigma and discriminated harm.

However, the increasing granularity of the data collection process, including longitudinal patient behavior tracking, geo-spatial patient traffic mapping, and the inclusion of pharmacy, insurance, laboratory, imaging, and genomic data, creates a heightened risk of privacy breaches.[36] Although the aggregation of these data types facilitates predictive analytics and optimisation of the health system, it also heightens the risks of patient re-identification, profiling, and secondary use of the

[30] A Jacoby and JK Austin, _Social Stigma for Adults and Children with Epilepsy‘ (2007) *Epilepsia* 48, 6–9.

[31] Emily Lenton _Health-Related Stigma: The Affordances of Electronic Health Management Systems in the Production of Structural Stigma‘ (2025) *Sociol Health Illn*, 47(4):e70043. <https://pmc.ncbi.nlm.nih.gov/articles/PMC12074563> accessed 8 January 2026.

[32] Ibid.

[33] Ibid.

[34] Ibid.

[35] E Goffman, *Stigma: Notes on the Management of Spoiled Identity*. (Simon and Schuster Inc, 1963)) <https://ia601503.us.archive.org/22/items/in.ernet.dli.2015.264015/2015.264015.Stigma.pdf> accessed 8 January 2026.

[36] Aniebe, (n 7).

health information.[37] The move from isolated medical records to health data systems changes the dynamics of health data governance from one of confidentiality to one of power and control.[38]

Data integrity in the health domain is more than just the concern of data confidentiality. Data integrity in the health domain includes completeness, accuracy, timeliness, validity, and security.[39] The weaknesses in any of these aspects of data integrity may compromise patient compliance, disease surveillance, and emergency response coordination.[40] In low-capacity systems, integrity weaknesses may imply that patients are unreachable, incorrectly classified, or excluded.[41]

3. Health Data Governance in Nigeria

a. Constitutional Foundation

The 1999 Constitution of the Federal Republic of Nigeria, in Section 37 guarantees the right to privacy of citizens, it provides: ―the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.‖ There is no express reference to personal health data or health information in the Constitution, however, in *Medical and Dental Practitioners Disciplinary Tribunal v Okonkwo*[42] the Supreme Court affirmed the importance of patient autonomy, privacy, and informed consent within the doctor–patient relationship, recognising that medical treatment must generally be based on the patient's consent. This constitutional framework provides a broad normative guarantee, leaving specific protection of health data to statutory and regulatory instruments.

b. **Nigeria Data Protection Act 2023**

The Nigerian Data Protection Act 2023 governs the processing of personal data in Nigeria. It recognises health data as _Sensitive Personal Data', which encompasses more stringent

[37] Ibid.
[38] Ibid.
[39] Tijani, (n 19) S229.
[40] Ibid, S230.
[41] Ibid, S226.
[42] (2001) 7 NWLR (Pt 711) 206 (SC)

obligations.[43] Under the NDPA, the processing of health data can only be done where there is consent, where it is necessary for the performance of an obligation of the data processor, or right of the data subject or where processing is carried out for medical care or community welfare, and done by or under the responsibility of a professional or similar service provider owing a duty of confidentiality among others. [44]

Health data may also be processed as a result of public health necessity, and scientific or statistical research grounded in law, which must be proportionate to the aim pursued.[45] The law requires that there must be specific measures to safeguard the fundamental rights and freedoms and the interests of the data subject. The Act also contains six data protection principles: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation and data security which are particularly relevant to health data.[46]

The Act also grants to data subjects such as right to access, rectify, erase, object to the processing of data, to withdraw consent, and right to data portability.[47] The NDPA 2023 also establishes the Nigeria Data Protection Commission (NDPC) also serves as the data protection authority responsible for investigating, enforcing and sanctioning.[48] By Section 28 of NDPA 2023, data controllers, including health establishments must carry out data protection impact assessments (DPIA) where processing will likely result in high risks to the rights and freedoms of data subjects (patients) before processing data. This means that any new health technology or a cloud-based EHR must undergo a DPIA to identify privacy risks before implementation. This ensures that protection of data in the Nigerian health sector takes a proactive stance as opposed to a reactive stance.

Section 24 of the NDPA 2023 provides that data controllers are to implement ‗appropriate technical and organisational measures' to ensure the security, confidentiality and integrity of data.[49] It lists the types of protection required, these include:[50] pseudonymisation which is

[43] NDPA 2023, s 65.
[44] Ibid, s 30.
[45] Ibid, s 30(1) (i).
[46] Ibid,s 2(a) – (f)
[47] Ibid, Part VI.
[48] Ibid, Part II.
[49] Ibid, s 24(2), 39(1).

basically _de-identification' of data cannot be linked to a person without additional information. It also includes encryption which is converting data into code to prevent unauthorized access, restoration system (restoring access to data in the event of physical or technical incident), regular testing, assessment and evaluation of the effectiveness of these security measures.

Such measures are likely to become especially relevant in light of the newly emerging Trusted Research Environments (TREs) in Nigeria, which aggregate de-identified health data from various sources, reportedly reaching hundreds of millions in total.[51] While these TREs are likely to make Nigeria an even more attractive location for pharmaceutical research and trial recruitment, they also imply the concentration of informational powers in data intermediaries.[52] The relevant question for the regulator becomes no longer whether health data is processed, but who controls access, on what basis, and with what level of transparency and auditing in place.

The prevalence of paper-based systems in various health facilities in Nigeria, coupled with a lack of technical knowledge and manpower, makes it difficult to comply with the complex NDPA system in the areas of monitoring, validation, and secure storage in real-time.[53] Although the use of digital forms has been introduced in some health facilities, various problems of accountability, validation, and misinterpretation persist unless the technological system is designed to promote compliance.[54]

The NDPA 2023 framework attempts to strike a balance between privacy protection and functional necessity. Routine clinical care is preserved through the medical-care exception;[55] emergency treatment is accommodated through the vital-interests ground;[56] and epidemiological surveillance and health research are enabled through public health and

[50] Ibid, s 39(2) (a, b, d, f).
[51] Aniebe, (n 7).
[52] Ibid.
[53] Tijani, (n 19) S232.
[54] Ibid.
[55] NDPA 2023, s 30(g).
[56] Ibid, s 30(c).

research provisions.[57] This accommodates the processing of health data for purposes such as disease control, digital health innovations and AI-driven diagnostics.[58] At the level of principle, the Act embodies a modern and risk-sensitive model of data protection that is in keeping with international best practices. At the level of sector-specific operationalisation, however, the framework is still under-elaborated. In the NDPA, critical concepts such as _substantial public interests,‘ _suitable and specific measures,‘ and _community welfare‘ are not sufficiently defined.

This raises critical concerns about the potential over-expansion of these exceptions. The broadly framed notions of —public interest‖ or —scientific research‖ may, if insufficiently scrutinised, gradually normalise secondary uses of sensitive health data.[59] Reliance on research exemptions may functionally dilute the centrality of explicit consent, thereby shifting informational control away from data subjects. The broad research exception raises questions about practical oversight. The NDPA does not contain detailed criteria with respect to anonymisation, secondary use limitations and ethical review. During the COVID-19 pandemic, there was a heightened sense of urgency around data-driven decision-making.[60] The role of automated outbreak management systems was highlighted by their ability to facilitate real-time reporting to the Nigeria Centre for Disease Control (NCDC), as well as triage based on risk criteria and digital contact tracing.[61] The pandemic, therefore, demonstrated how public health crises can speed up centralisation and integration of data systems, without necessarily developing parallel oversight of data proportionality, retention, or secondary use.

Although the Act provides a robust framework for protecting health data by classifying it under the highest level of data sensitivity and applying a regulatory framework to process it under certain conditions, it is submitted that its effectiveness extends beyond the presence of exceptions under the Act. It depends on regulatory guidance, oversight and the enforcement

[57] Ibid, s 30(i).

[58] European Commission _Artificial Intelligence in Healthcare‘ < https://health.ec.europa.eu/ehealth-digital-health-and-care/artificial-intelligence-healthcare_en> accessed 16 February 2026.

[59] _Secondary use of health data refers to a regulatory framework that supports using health data for other purposes than it was originally created and collected for.‘: Remedybytes, _Secondary Use of Health Data‘ < https://remedybytes.com/secondary-use-of-health-data/> accessed 18 February 2026; Tsaone Tamuhla and others, _Multiple Modes of Data Sharing Can Facilitate Secondary Use of Sensitive Health Data‘ (2023) *BMJ Global Health* 8, e013092. doi:10.1136/bmjgh-2023-013092.

[60] Tijani, (n 19) S227.

[61] Ibid, S230.

capacity of the authorised bodies. The classification of health data under _sensitive data‘ is a crucial step in protecting health data in Nigeria‘s digital health space; however, it is not enough. The distinctions between identified, pseudonymised, and anonymised health data are crucial to the Nigerian regulatory landscape as each state of data carries different levels of risk regarding patient privacy and potential discrimination.

c. The General Application and Implementation Directive (GAID)

The Nigeria Data Protection Commission (NDPC) is a statutory commission with the power to issue binding directives, such as the General Application and Implementation Directive (GAID) 2025.[62] The General Application and Implementation Directive (GAID) operationalises statutory protections applicable to health data by clarifying compliance expectations, supervisory procedures, and sector-sensitive safeguards. Although GAID is horizontally applicable, several of its provisions directly affect the governance of health data. It reinforces the NDPA‘s classification of health data and genetic information as sensitive personal data, thereby subjecting it to enhanced lawful processing requirements.[63] The Directive allows for the processing of health data without consent when it is necessary for the preservation of life or livelihood, particularly in emergency medical situations where the data subject cannot provide consent.[64] It permits data processing during public health or humanitarian emergencies,[65] and mandates a DPIA for any processing involving "sensitive personal data" (such as medical records) or where software is deployed to process such datasets.[66] Article 4 mandates that the Nigeria Data Protection Commission (NDPC) must cooperate with other public authorities (such as the Ministry of Health) to develop sectoral guidelines, ensuring that any specific health data rules do not negate the objectives of the NDP Act. If health data is being transferred outside Nigeria, the NDPC may require the approval of a Cross-Border Data Transfer Instrument (CBDTI).[67] The Commission may consider the results of a compliance audit before granting this

[62] NDPA 2023, s 6(c); Nigeria Data Protection Act (NDP ACT) 2023 General Application and Implementation Directive (GAID) 2025 NDPC/NDP ACT-GAID/01/2025 <https://ndpc.gov.ng/wp-content/uploads/2025/07/NDP-ACT-GAID-2025-MARCH-20TH.pdf> accessed 10 January 2026

[63] Ibid, art 18(1)(b).

[64] Ibid, art 24.

[65] Ibid, art 25.

[66] Ibid, art 28(3)(l) & (8)

[67] Ibid, schedule 5, para 1(b).

approval.[68] The GAID bridges the gap between data law and research ethics by prioritizing Data Ethics (Article 41) and requiring that any processing for the "public interest" must be necessary and proportionate to the aim pursued.

e. National Health Act 2014[69]

Health data governance is also regulated by other sector-specific statutes and professional regulations. For instance, there is the National Health Act 2014 which provides in Section 26 (1) that patient information relating to his or her health status, treatment or stay in a health establishment not be disclosed. Such information can only be disclosed where the patient consents, or there is a court order, with respect to children or persons unable to give consent: with the request of the guardian or representative, on grounds of danger to public health.[70] The information may also be disclosed where it is in the interest of the patient.[71] The National Health Act contains extensive rules on data integrity and access control. The Act also obligates the person in charge of the health establishment to take measures to ensure that there is no unauthorised access to the records or storage facilities where records are kept.[72] A person who fails to perform this obligation, or falsifies a patient‘s data, wrongfully destroys a patient‘s record, fails to create or carry out a change to a patient‘s data when required to do so, is guilty of an offence and is punishable with two years‘ imprisonment or a fine of ₦250 000.[73] It prohibits giving false information with the intention that it be put into a record, copying any part of a patient‘s record without authority, linking any part of a computer system in which records are kept to another computer or electronic system without authority, destroying, copying, or modifying record-keeping software without authority.[74] It also criminalises revealing a patient‘s identity by connecting it to their medical condition without authority, as well as general hacking

[68] Ibid, schedule 5, para 5.
[69] Federal Republic of Nigeria Official Gazette No. 145 Lagos - 27th October, 2014 Vol. 101 Government Notice No. 208
[70] Ibid, s 26(1), (2).
[71] Ibid, s 27.
[72] Ibid, s 29(1).
[73] Ibid.
[74] Ibid.

of a record or record-keeping system or interception of information.[75] The Act also criminalises unauthorised networking of systems or impairing the systems used for health data.[76] These offences carry a penalty of imprisonment for a term not exceeding two years or a fine of ₦250, 000.

The National Health Act contains very clear sanctions for tampering with health data which include offenses such as falsification or unauthorised access; it focuses more on individuals than institutions. The fine of N250, 000 may be an insufficient deterrent for large-scale digital health platforms or corporate entities handling massive volume of' Health Big Data. A large Health Maintenance Organisation (HMO) or a multinational technology provider may consider the fine as a _cost of doing business' rather than an incentive to invest in high-level cybersecurity. The reason for this penalty may be because the National Health Act was enacted at the time when _Big Data' was not a mainstream regulatory concern in Nigeria. The NDPA 2023 contains stricter penalties for institutional failures: the penalty may be up to ₦10 Million or 2% of annual gross revenue (whichever is higher).[77] The linkage of fines to gross revenue ensures that organisations take data protection as seriously as their profit margins. The NDPC has been actively enforcing the penalties, in 2024; it issued a fine of ₦555 Million to a bank for data processing violations.[78] In fact, the NDPC recently reported collecting over ₦7.2 billion (approximately $5.1 million at exchange rates as at February 2026) as penalties.[79] Within the context of health data, the NDPC's ability to levy hefty fines of up to ₦10 million or 2% of the yearly revenue for data controllers is an important check on the influence of large HMOs and public health organisations.[80] By ensuring that there is a clear procedure for the reporting of breaches of privacy, the NDPA 2023 gives effect to the right to privacy as provided in Section 37 of the 1999 Constitution, ensuring that accountability is not only a policy objective but also a justiciable reality.[81]

---

[75] Ibis, s 29(2(g) and (h).
[76] Ibid, s 29 (i) and (j).
[77] NDPA 2023, s 48(4).
[78] One Trust Data Guidance _Nigeria: NDPC fines Fidelity Bank NGN 555.8M for Data Processing Violations' Mhttps://www.dataguidance.com/news/nigeria-ndpc-fines-fidelity-bank-ngn-5558m-data> accessed 11 February 2026.
[79] Fatima Oladunni _Nigeria Just Collected ₦7.2 Billion in Data Privacy Penalties—And It's Just Getting Started' Techmonshot, February 10 2026, <https://techmoonshot.com/2026/02/10/nigeria-just-collected-%e2%82%a67-2-billion-in-data-privacy-penalties-and-its-just-getting-started/> accessed 11 February 2026.
[80] NDPA 2023, s 48(4).
[81] Ibid, s 40.

Nigerian medical ethics, which are founded on principles of duty of care, duty to avoid harm, and autonomy, emphasize privacy as a medical ethical responsibility.[82] The Nigerian Medical Association (NMA) and the Medical and Dental Council of Nigeria (MDCN) developed guidelines for health care practitioners on confidentiality and privacy.[83]

4. Fragmentation and Regulatory Gaps

Despite the existence of multiple protective instruments, the governance landscape is not structurally unified. The legal framework for health data in Nigeria is fragmented[84] due to the presence of constitutional standards, general data protection law, sector specific health legislation, and professional ethical standards. This creates a situation of overlapping obligations without a unified governance structure. This system engenders regulatory overlap without integration. The NDPA prescribes compliance obligations at the institutional level but fails to set up operational standards at the health sector level. The National Health Act prescribes confidentiality obligations and criminalizes violations but fails to integrate contemporary data protection principles such as thresholds for pseudonymisation, secondary use compatibility, and algorithmic accountability. Professional ethics, such as medical confidentiality codes, apply outside the NDPC's enforcement framework. Public health emergency powers facilitate rapid data collection but lack proportionality review structures.

Fragmentation is evident at the institutional level. The NDPC monitors data protection compliance in general, while the Federal Ministry of Health acts within its respective legal frameworks. There is no formalised system to ensure that data protection compliance is integrated. This fragmentation becomes evident in contexts such as: use of health datasets for AI training, for research among others. For instance, AI deployment in Nigeria depends on large-scale data aggregation in a context where datasets remain fragmented and regulatory enforcement is inconsistent.[85]

---

[82] Ottah, and Imoisi, (n28) 6.

[83] Ibrahim Sulaiman, *Medical Ethics in Nigerian Practice: Legal and Professional Perspectives* (University Press, Ibadan 2019) 67.

[84] Ottah, and Imoisi, (n28) 9.

[85] Miracle Okwukwu and others, _Artificial Intelligence in Nigeria Healthcare: A Review of State, Challenges and Opportunities' (2025) *EthAIca* 4:210 DOI:10.56294/ai2025210

Health data governance in Nigeria is faced with a number of challenges that are interlinked: there is a huge gap in the technological infrastructure, as most of the health institutions lack the contemporary technological framework that would enable them to handle the sensitive data of the patients.[86] There is also a huge shortage of human resources with expertise in cybersecurity and data privacy.[87] The level of enforcement remains patchy, especially in resource-constrained health facilities and digital health platforms.[88]

Moreover, fragmentation leads to disparities in enforcement. Large private hospitals and health tech companies may have compliance teams that can carry out DPIAs, encryption audits, and breach notifications. On the other hand, public hospitals, which are often underfunded and transitioning from paper-based systems, may not have the capacity to enforce ―appropriate technical and organisational measures‖ as mandated by the NDPA.[89] Thus, a two-tier privacy system emerges, where rights exist but are operationally uneven.

Normative fragmentation is equally apparent in the treatment of research and public interest exceptions. The NDPA permits processing for public health and scientific research where grounded in law and accompanied by suitable safeguards. Yet these safeguards are not elaborated in the statute. The absence of detailed anonymisation standards, compatibility tests, or structured prior authorisation mechanisms contrasts with regimes such as the GDPR, which embeds defined authorisation procedures and regulator involvement for high-risk processing. The consequence is a governance model that is formally robust but structurally disjointed. Without greater regulatory coordination, clearer delineation of responsibilities, and sector-specific elaboration of safeguards, fragmentation risks undermining both privacy protection and the effective fulfilment of the right to health.

Addressing fragmentation therefore requires more than legislative amendment; it demands institutional integration, detailed regulatory guidance, and structured oversight mechanisms capable of aligning privacy, public health, and innovation within a coherent rights-based framework. It is important to note that the GAID 2025 acts as an anchor that forces all other

[86] Ibid, 3.
[87] Ibid.
[88] Ibid 4, 7; Samuel N. Ibenegbu, *Health care and the Law: A Nigerian Perspective* (LexisNexis, 2021) 91.
[89] Recent studies reveal that _many public institutions, especially in healthcare, lack the necessary technological infrastructure to store and manage data securely and efficiently.‘ See Ayomipo Alademehin _Enhancing Data Governance in Nigeria: A Strategic Framework for National Development, with a Focus on Healthcare‘ (February 05, 2025). < http://dx.doi.org/10.2139/ssrn.5124913> accessed 10 January 2026

regulations to align. It mitigates fragmentation by providing a single supremacy rule in Article 3 and a formal collaboration mechanism in Article 4 to ensure that health data governance is consistent across all Nigerian institutions. It is important to note that the GAID mitigates fragmentation at the data protection level, but does not structurally integrate the entire health governance architecture. It mitigates certain interpretive and supervisory gaps within the data protection framework, without integrating the broader constitutional, sectoral, and institutional landscape.

5. Comparative Analysis

Health data processing in Nigeria is also impacted by public health and research imperatives. During disease outbreaks or public health emergencies, data collection and sharing may be justified under statutory powers vested in public health authorities. For example, during the COVID-19 pandemic, a research collaboration effort involving the Nigerian Institute of Medical Research resulted in the development of an outbreak management system that aimed to enhance the completeness, accuracy, and validation of data at testing sites.[90] This ensured that the health data used for pandemic control was valid for research assessment. However, Nigeria lacks a detailed legal framework specifying proportionality, safeguards, or oversight mechanisms for such exceptional processing, creating risks of overreach. Comparative experience illustrates how similar constitutional democracies have attempted to structurally integrate health data governance.

a. Comparative Insights and Lessons for Nigeria

This paper uses South Africa as a comparator for Nigeria in this context because both jurisdictions are constitutional democracies with entrenched privacy guarantees and public-private health systems marked by structural inequality. Like Nigeria, South Africa operates a structurally unequal dual public–private healthcare system,[91] in which both state institutions and

[90] Tijani, (n 19).

[91] SG Abbott and C Sigamoney , _The Current Healthcare Industry in South Africa‘ *(2024) International Journal of Health and Psychology Research*, 12(3), 11-36.

private actors play significant roles in service delivery and digital health innovation.[92] Both countries are also experiencing rapid digitisation of healthcare delivery.[93] South Africa has a well-established regime for health data under the Protection of Personal Information Act (POPIA) 2013.[94] Its framework offers a regional model that is both rights-based and socio-economically comparable; this makes the analysis normatively instructive yet contextually realistic.

Section 14 of the South African Constitution[95] protects the right to privacy and judicial interpretation has recognised informational privacy as part of this protection. South Africa's constitutional jurisprudence has more clearly articulated informational self-determination as an aspect of dignity.[96]

Under POPIA, the conditions for lawful processing are codified in Chapter 3 (Sections 8–25), including: accountability, processing limitation, purpose specification among others. Section 22 of POPIA imposes a clear statutory obligation to notify both the regulator and affected data subjects of security compromises. POPIA also introduces prior authorisation requirements under Section 57 for certain high-risk processing activities, thereby strengthening ex ante regulatory oversight. Nigeria's NDPA requires Data Protection Impact Assessments (Section 28), but structured prior consultation with the regulator is less clearly institutionalised.

Under the POPIA, health data is categorised as _special personal information.' In Section 26, it establishes a general prohibition on processing special personal information. There are however exceptions, such as where processing is carried with the consent of the data subject, necessary for the establishment or defence of a right, or to comply with a legal obligation.[97] The prohibition

---

[92] Jonathan Klaaren and Firoz Cachalia, _A South African Public Law Perspective on Digitalisation in the Health Sector' (2021) 15 *Digital Pathway Paper Series,* 6 <https://www.researchgate.net/publication/354355061_A_South_African_Public_Law_Perspective_on_Digitalisation_in_the_Health_Sector#:~:text=We%20made%20two%20further,public%20and%20private%20actors)%20and> accessed 16 February 2026.

[93] Ibid, 3.

[94] Protection of Personal Information Act 4 of 2013, <https://popia.co.za/> accessed 16 February 2026.

[95] As adopted on 8 May 1996 and amended on 11 October 1996 by the Constitutional Assembly, < https://www.justice.gov.za/constitution/SAConstitution-web-eng.pdf> accessed 16 February 2026.

[96] J Neethling, _The Concept of Privacy in South African Law' (2005) *South African Law Journal* 122(1) < https://hdl.handle.net/10520/EJC53620> accessed 12 January 2026

[97] POPIA 2013, s 27.

does not apply to processing for historical, statistical or research purposes, provides that it is under the following conditions: [98]

2 The processing serves the public interest and the data processing is a necessary part of achieving that goal.

3 It is genuinely impossible or extremely difficult to obtain the data subject's consent. However, strong protections must be put in place to ensure data subject's privacy is not harmed to a disproportionate extent.

4 Where the data subject intentionally made the information public themselves.

5 The processing follows the specific rules and requirements laid out in sections 28 through 33 of this law.

The Information Regulator has power to authorise any party to process special personal information upon application by that party, if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the data subject.[99] The Regulator is also empowered to impose reasonable conditions in respect of any authorisation granted.[100]

Under Section 32, the prohibition does not apply to processing by medical professionals, healthcare institutions or facilities or social services done in the course of their duties.[101] This Section also regulates processing by insurance companies, medical schemes, medical scheme administrators, healthcare organisations, schools, public bodies, administrative bodies, requiring that such processing be subject to a duty of confidentiality.[102] Under the Act, with regard to the processing of information for historical, statistical, or research purposes, the responsible party must ensure that the subsequent processing of information is compatible with the purpose for which the information was collected and will not be published in an identifiable form. [103]

While both the NDPA 2023 and the POPIA 2013 recognise exceptions for public interest and research, the POPIA embeds the exceptions within a more granular statutory architecture. It

[98] Ibid, s 27 (1) (a-e).
[99] Ibid, s27(2).
[100] Ibid, s 27(3).
[101] Ibid, s 32(1) (a).
[102] Ibid, s 32(2).
[103] Ibid, s 15 (3) (e).

specifically links special category processing to defined authorisations, compatibility requirements and operator-level confidentiality obligations.

The NDPA does not define anonymisation thresholds, or mandatory linkage with institutional review boards. In a context of increasing AI-driven health analytics, this regulatory silence is significant.

b. The Legal Framework for Health Data for Research Purposes under the European Union General Data Protection[104]

According to the European Union's legal framework, health and genetic data are considered special categories of personal data, as defined in the General Data Protection Regulation (GDPR). Article 9(1) establishes a default rule that the processing of this category of data is prohibited. Processing is only permissible where one of the grounds identified under Article 9(2) applies, including situations involving explicit consent, considerations of substantial public interest, public health purposes, or scientific research activities.[105] The research and public health exceptions under Article 9(2) (i) and (j) are not self-standing authorisations. They operate in conjunction with Article 89 GDPR, which requires ―appropriate safeguards,‖ including data minimisation and technical or organisational protections such as pseudonymisation.

Although the NDPA considers health data to be sensitive personal data and allows for the processing of such data on the basis of public interest and research, it fails to outline a conditional framework as elaborate as that in the GDPR. Contrary to the GDPR, the NDPA fails to incorporate a proportionality review at the special category data provision level and fails to outline statutory requirements akin to the Article 89 safeguard framework. The lack of elaborate legislative requirements on pseudonymisation standards, re-identification risk mitigation, and mandatory data protection impact assessments in research settings could potentially broaden the scope of public interest processing.

[104] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1. (hereafter referred to as GDPR).

[105] GDPR 2016, art 9(2)(a), art 9(2)(g), art 9(2)(i), art 9(2)(j).

6. Strengthening the "Right to Health" through the AAAQ Framework

While comparative analysis reveals institutional design differences, the ultimate normative test remains whether Nigeria's framework advances or undermines the substantive right to health. The right to health is recognised under several international instruments such as the International Covenant on Economic, Social and Cultural Rights (ICESCR);[106] the United Declaration of Human Rights,[107] the _International Convention on the Elimination of All Forms of Racial Discrimination (CERD);[108] among others. The African Charter on Human and Peoples' Rights also guarantees the right to health.[109] The 1999 Constitution of Nigeria in Chapter II also provides for the right to health.[110] The right to health is broader than mere availability of healthcare facilities. It includes entitlement to relevant health education and information, together with the opportunity to participate actively in health-related decision-making processes.[111] In its authoritative interpretation of the right to health in General Comment No. 14,[112] the UN Committee on Economic, Social and Cultural Rights articulated the normative content of the right through what has become known as the AAAQ framework. This framework identifies four interdependent and indivisible elements: availability, accessibility, acceptability, and quality.[113]

These elements are not only applicable in the provision of health care but also relate to the overall factors that influence health outcomes, including access to safe water, sanitation, proper

[106] ICESCR, art 12.
[107] *U*niversal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) (UDHR) art 25.
[108] The International Convention on the Elimination of All Forms of Racial Discrimination (CERD) (1965), art 5. adopted 21 December 1965 BY UN General Assembly resolution 2106 (XX), <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial> accessed 16 February 2026.
[109] The African Charter on Human and Peoples' Right, African Charter on Human and Peoples' Rights, adopted June 27, 1981, O.A.U. Doc. CAB/LEG/67/3/Rev.5, 21 I.L.M. 58 (1982), entered into force Oct. 21, 1986, art 16
[110] Constitution of the Federal Republic of Nigeria, 1999 (as amended).
[111] UN Committee on Economic, Social and Cultural Rights (CESCR), _General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12)' (11 August 2000) UN Doc E/C.12/2000/4.
[112] General comment no. 14 (2000), The right to the highest attainable standard of health (article 12 of the International Covenant on Economic, Social and Cultural Rights) UN. Committee on Economic, Social and Cultural Rights (22nd sess. : 2000 : Geneva) 2000 < https://digitallibrary.un.org/record/425041?ln=en&v=pdf> accessed 16 February 2026.
[113] Ibid, para 12.

nutrition, housing, health education, and access to health information..[114] It includes the "right to seek, receive and impart information and ideas concerning health issues."[115] It is worthy of note that the right to receive information cannot justify practices that erode the duty to maintain the confidentiality of personal data.[116] Health data governance in Nigeria can be meaningfully assessed through the AAAQ framework**:** Availability, Accessibility, Acceptability, and Quality. Although the Nigeria Data Protection Act, 2023 (NDPA) provides a legal framework for the protection of sensitive health information, its role in the realisation of the right to health must be critically assessed through the AAAQ framework

Availability means that health facilities, goods and services, such as hospitals, clinics must be available.[117] Ensuring accessibility means that all individuals can use health facilities, products, and services without discrimination, including having physical access, reasonable costs, and access to necessary health-related information.[118] Acceptability is concerned with respect for the principles of medical ethics and confidentiality. If exceptions in respect of research and public interest are not subject to strict scrutiny, oversight, patient trust could be undermined. Accessibility (Non-discrimination) is at issue where research data is reused for profiling or predictive analytics purposes without sufficient protection against discrimination. Vulnerable groups are likely to be disproportionately affected by surveillance or exclusionary algorithmic decisions.[119]

Acceptability means that these facilities and services should function within the framework of medical ethics and be culturally sensitive, considering variations in gender, age, and social settings.[120] This implies that they should be respectful of the cultures of persons, minorities, peoples, and communities; take into account the differences between genders and the needs that arise at different stages of life; and be structured in a manner that ensures confidentiality while enhancing the health and well-being of the people they serve. This lack of definition of key

[114] Ibid, para 11.
[115] Ibid, para 12.
[116] Ibid.
[117] Ibid, para 12 (a).
[118] Ibid, para 12(b).
[119] Cecil Abungu, _Algorithmic Decision-Making and Discrimination in Developing Countries _ (2021 – 2022) *Journal of Law, Technology & The Internet* 13(1), 46.
[120] Ibid, para 12(c).

concepts such as public interest, substantial interest, in the NDPA 2023, provides for broad administrative discretion. In the health data context, especially for HIV status, reproductive health data, genetic data, and epidemiological data, this could lead to a lack of acceptability, as patients cannot readily foresee how their data will be used outside the medical setting.

Quality means that health facilities, goods and services must ‗be scientifically and medically appropriate and of good quality.'[121] Quality may also be affected where data is reused without accountability, as patients may not provide accurate information to healthcare providers out of concern for secondary use.

Health data governance in Nigeria is at the nexus of privacy law, public health policy, and human rights obligations. When evaluated through the lens of the AAAQ criteria of Availability, Accessibility, Acceptability, and Quality, it is clear that mere legal compliance is not enough. The real test of health data governance is whether it can build public trust, avoid discrimination, help with evidence-based planning, and ensure that the digital health infrastructure improves, rather than undermines, the effective enjoyment of the right to health. A rights-based approach, therefore, requires not only progressive regulation but also a focus on procedural integrity, balanced limitations on exceptions, open accountability, and sustained regulatory strength. Otherwise, health data governance may be progressive in form but weak in substance.

7. Recommendations

In Nigeria, the framework of health data governance could be improved by a more targeted approach to institutional development, rather than a complete legislative reform. Firstly, proportionality should be given a concrete definition through the imposition of mandatory documented necessity and proportionality assessments, especially in the context of large-scale, AI-based, or secondary research processing of health data. Secondly, exemptions for research and public interest should be given more concrete statutory definitions to ensure that consent and informational autonomy are not gradually diminished; this includes more specific standards for compatibility, ethical assessment, and anonymisation. Thirdly, the Nigeria Data Protection Commission must issue compulsory technical guidance on anonymisation and de-identification to reduce the risks of re-identification. Fourthly, the challenge of regulatory fragmentation can be

[121] Ibid, para 12(d).

addressed by harmonized regulatory guidance from the data protection regulatory authority and health regulators to ensure supervisory competence and compliance standards. Finally, there should be a consideration for the introduction of prior authorisation requirements for high-risk health data processing and improved remedies for data subjects.

8. Conclusion

The health data governance framework in Nigeria is characterized by significant legislative development but is still imbalanced in its structure. The Nigeria Data Protection Act (NDPA) is a strongly normatively grounded and rights-focused basis for the protection of sensitive health data. Nevertheless, as has been illustrated in this article, normative strength is not a sufficient basis for effectiveness. There are still gaps in the area of proportionality, research exemptions, and anonymisation.

The comparative analysis with South Africa‘s POPIA and the European Union‘s GDPR further demonstrates that effective health data governance requires more than broad rights-based guarantees. Both frameworks provide more structured oversight mechanisms for high-risk processing, clearer proportionality safeguards, stronger authorisation procedures, and more detailed regulation of research-related processing and anonymisation standards. These comparative insights illustrate that Nigeria‘s challenge is not the absence of a legal framework, but the need for greater institutional integration, sector-specific operational safeguards, and clearer procedural limitations capable of balancing innovation, public health objectives, and informational privacy.

Although the General Application and Implementation Directive (GAID) reduces some of the interpretative uncertainties, it does not, however, address the issue of fragmentation in the health data regulatory framework. Accordingly, the priority for Nigeria is not the creation of an entirely new legal regime, but the strengthening of institutional coordination, procedural safeguards, and sector-specific oversight mechanisms. Improving proportionality review, high-risk processing oversight, and regulatory coordination would help address fragmentation without undermining the underlying framework established by the NDPA. In this regard, therefore, the issue of health data governance in Nigeria needs to be addressed through structural adjustments to ensure that innovation and public health goals continue to be consistent with privacy, dignity, and human rights.