July - December 2025 Volume 34 Issue 2
PRINT ISSN: 2277-1867
ONLINE ISSN: 2277-8853

JOURNAL OF FORENSIC MEDICINE SCIENCE AND LAW

Official Publication of Medicolegal Association of Maharashtra

MULTISPECIALITY, MULTIDISCIPLINARY, NATIONAL
PEER REVIEWED, OPEN ACCESS, MLAM (SOCIETY) JOURNAL
Indexed with Scopus (Elsevier)

Editorial Office Address
Department of Forensic Medicine & Toxicology, Third Floor, Mortuary Building, Lokmanya Tilak Municipal Medical College & LTMG Hospital, Sion, Mumbai, Maharashtra, India. Pin-400 022. Email id: mlameditor@gmail.com Phone: 022-68660000/ +91-9423016325.

JOURNAL OF FORENSIC MEDICINE SCIENCE AND LAW
(Official Publication of Medicolegal Association of Maharashtra)
Email.id: mlameditor@gmail.com

PRINT ISSN: 2277-1867
ONLINE ISSN: 2277-8853

Review Article

From Hippocratic Oath to Digital Sovereignty: Legislating Patient Data Rights and Protection in Nigeria and India

Chinyere C Ogah[a], Chuks Molokwu[b], Princess Chinyere Ngene[c], Victor C Aneke[c], Hemen P Faga[d]*
[a]Senior Lecturer, [d]Professor, Faculty of Law, Ebonyi State University, Abakaliki, Nigeria. [b]Lecturer, Department of Forensic Science, Federal University of Technology, Owerri, Nigeria. [c]Lecturer, David Umahi Federal University of Health Sciences, Uburu, Nigeria.

Article Info

Received on: 06.09.2024
Accepted on: 25.10.2025

Key words
Data protection,
Patient rights,
Data sovereignty,
Medical records,
Digital privacy.

Abstract

Introduction: In the digital age, the data subject is increasingly empowered to control and determine the uses of information relating to his digital identity. Medical records have gradually transcended their physical form into sensitive digital data. **Objective:** This paper examines the current state of legal frameworks in Nigeria and India protecting this sensitive data and its governance vis-à-vis the patient's right of data sovereignty**. Methodology:** Using the doctrinal black-letter approach, which includes primary and secondary sources, the paper examines the governance of sensitive health data under the Nigeria Data Protection Act (NDPA) 2023 and India's Digital Personal Data Protection Act (DPDPA) 2023 to determine if patients in the two jurisdictions have attained digital sovereignty, and analyses how these jurisdictions balance the sanctity of medical confidentiality and patient data sovereignty. **Results and Discussion:** It argues that while India has developed a robust jurisprudence recognizing patient data rights through consumer protection law, Nigeria's approach was historically restrictive, finding that the enactment of the NDPA 2023 represents a seismic shift, potentially bringing Nigeria's statutory framework in line with modern data protection principles and, in some aspects, surpassing India's yet-to-be-fully-implemented DPDPA 2023. **Conclusion:** The paper concludes that both nations are on a convergent path towards empowering patients as data subjects, but success hinges on effective implementation, robust enforcement, and cultural change within healthcare institutions.

1. Introduction

A patient's journey through the healthcare system leaves a digital and paper trail—a narrative of vulnerability, hope, diagnosis, and treatment. This narrative encapsulated in the medical record,

How to cite this article: Ogah CC, Molokwu C, Ngene PC, Aneke VC, Faga HP. From Hippocratic Oath to Digital Sovereignty: Legislating Patient Data Rights and Protection in Nigeria and India. J Forensic Med Sci Law. 2025;34(2):57-62. doi: 10.59988/jfmsl.vol.34issue2.11

***Corresponding author:** Hemen P. Faga, Professor, Faculty of Law, Ebonyi State University, Abakaliki, Nigeria.
Email: hemenfaga@gmail.com

is more than a clinical tool; it is a profound repository of personal data, intimately detailing the patient's biological data and vulnerabilities.[1] Historically, this dossier was treated as the exclusive property of the healthcare institution, a secret ledger locked away from the very person it described.[2] The patient was a subject of the record, not its owner.

Today, a global revolution in data protection challenges this paternalistic model. The concept of 'information self-determination' posits that individuals have a fundamental right to control their personal data.[3] a category in which health information is arguably the most sensitive. This paper explores the tumultuous journey towards recognizing this right in two of the developing world's largest democracies: **Nigeria and India**. Both nations share interesting similarities: an expanding population; a rapidly digitalizing healthcare sector, and a history of relegating patient access to medical records to a privilege, rather than a right.[4]

This paper delves into the legal history, judicial activism, and regulatory challenges that define the battle for patient data sovereignty. It examines Nigeria's transformative Data Protection Act (NDPA) 2023 against India's revolutionary Digital Personal Data Protection Act (DPDPA) 2023 and the complex tapestry of medical ethics and consumer law, to answer the following questions: have patients in both countries attained digital sovereignty in the protection and governance of their personal health data? What are the gaps evident in Nigeria and India's data protection legal framework for the protection and governance of patients' personal health data? How can these gaps be remedied drawing from the provisions of each country's data protection regime?
In order to answer these questions, the paper is divided into eight sections. Section 2 explains the research methodology. Sections 3 and 4 establishes the special status of health data and the critical balance between confidentiality and the governance of health data in Nigeria and India. Section 5 examines Nigeria's transformative journey from a paternalistic model to the rights-based paradigm of the Nigeria Data Protection Act (NDPA) 2023, while section 6 traces India's development of patient rights through robust consumer jurisprudence underpinned by the Digital Personal Data Protection Act (DPDPA) 2023.

Section 7 offers a structured comparative analysis of both regimes in Nigeria and India, evaluating the rights and gaps for the protection and governance of personal health data. Section 8 contains the conclusion and recommendations for both countries to achieve genuine patient data sovereignty through effective enforcement, cultural change, and legal harmonization.

2. Method

The paper adopts a comparative legal research method utilizing the doctrinal black-letter approach to analyze the primary legislative frameworks of Nigeria's Data Protection Act (NDPA) 2023 and India's Digital Personal Data Protection Act (DPDPA) 2023. The research involves a critical analysis of these statutes and regulatory guidelines, supplemented by secondary sources including scholarly journal articles, books, online sources and case law. The objective is to systematically compare the provisions for patient data rights, identify regulatory gaps, and evaluate the efficacy of each legal regime in transitioning from traditional medical confidentiality to a modern framework of digital data sovereignty, thereby assessing their alignment with global data protection standards.

3. Medical Data: Why It Demands Special Protection

Medical data encompasses a wide spectrum of information, from genetic blueprints and biometric data to medical history, diagnosis, and treatment notes.[5] It can reveal not just current health status of a patient but also future vulnerabilities, family lineages, and deeply private aspects of one's life. The sensitivity of this data creates a dual imperative:

a. Protection: it must be shielded from unauthorized access, misuse, and discrimination. A data breach involving health information can have devastating consequences, from social stigma to insurance denial and employment discrimination.
b. Access: the data subject—the patient—must have the ability to access, understand, and utilise this information for their own care, continuity of treatment, and empowerment.

In both Nigeria and India, the transition from paper-based to electronic health records (EHRs) has amplified these imperatives.[6] Digitisation offers immense benefits for healthcare delivery but also magnifies the risks of data misuse and the critical need for robust legal safeguards.

4. Confidentiality, Trust, and the Governance of Health Data in Nigeria and India

There is a veiled connection between the time-honored principle of confidentiality and data self-determination of patients.[7] Historically, the ethical duty of confidentiality enshrined in professional codes like the Medical and Dental Council of Nigeria

(MDCN) Code of Medical Ethics[8] and the Medical Council of India (MCI) Regulations,[9] is the bedrock of therapeutic alliances. However, the digital revolution has fundamentally reshaped this matrix such that the patient's narrative is no longer confined to handwritten notes in a dusty file, but now transformed into structured digital data that can be copied, stored, analyzed, and shared across continents in milliseconds. Therefore, for the patient to retain control of health data, this transformation demands a parallel evolution of the traditional, albeit crucial, ethical duty of confidentiality, towards a more robust, comprehensive governance structure for the entire lifecycle of data processing. This encompasses not just the final act of disclosure, but every step including the initial collection, its storage security, the myriad uses, and the potential transfer to third parties.[10,11]

Such shift creates a critical tension, particularly in the realm of secondary data use—using health data for purposes beyond the immediate clinical care of the individual patient,[12] extending to vital endeavors like biomedical research, public health surveillance, epidemiological studies, and healthcare system planning. Indeed, in vast and diverse nations such as Nigeria and India, the potential benefits of aggregated health data could be staggering; it may help track the spread of infectious diseases, identify risk factors for non-communicable diseases like diabetes and hypertension, and ultimately develop more effective, personalized treatments tailored to their unique populations.[13]

The ethical and legal challenge of the digital revolution vis-à-vis confidentiality and data self-determination of patients is striking a balance between the public good and the individual's right to privacy and autonomy. This can be achieved through implementing principled safeguards, such as:

a. Anonymisation and Pseudonymisation*:* the former (Anonymisation) irreversibly strips data of all direct and indirect identifiers and effectively removes the data from the scope of privacy laws.[14] The latter (Pseudonymisation) on the other hand, replaces identifying fields with artificial identifiers, which offers a practical middle ground. Both principles protect patient identity while allowing researchers to link data points meaningfully.[15]
b. Purpose Limitation and Data Minimisation*:* purpose limitation mandates that data collected for one specific purpose (e.g., treating malaria) should not be arbitrarily repurposed for another (e.g., marketing insurance products) without further authorisation.[16] Data minimisation requires that only data that is strictly *necessary* for the stated purpose is collected. This prevents the hoarding of excessive, sensitive information, thereby reducing the risk and impact of potential data breaches.[17]

The legal landscape in both Nigeria and India increasingly reflects this sophisticated approach. The era of relying on broad implied consent—where a patient's mere presence in a hospital was sufficient consent to any future use of their data—has ended. Nigeria and India's new data protection laws, the NDPA (2023) and DPDPA (2023), pushes towards models where patients are informed about how their data would be used for secondary purposes, and their consent explicitly and specifically required for such activities.[18]

This seismic shift transforms the patient from a passive subject of data collection into an informed participant in the health data ecosystem, with the right to know how his digital double is being used to advance medicine, and the power to consent to that noble cause.[19]The balance between harnessing the incredible power of health data for the greater good and protecting individual privacy is the defining challenge of modern medical ethics in the digital age.

5. The Nigerian Landscape: From Paternalistic Custodianship to Data Subject Empowerment

5.1 The Pre-NDPA 2023 Era: A Regulatory Vacuum

Prior to 2023, Nigeria's legal framework for medical data protection was strikingly anachronistic.[20] The MDCN Code of Medical Ethics 2008 and sections 27-29 of the National Health Act (NHA) 2014 placed the ownership and control of medical records firmly with healthcare providers.[21] Paragraph 44 of the MDCN Code explicitly stated that records were "not for the consumption of any person who is not a member of the profession". Patients seeking their records for litigation or second opinions faced a wall of institutional resistance, often having to resort to costly court orders for disclosure.[22] This created a profound power imbalance, leaving patients unable to verify the accuracy of their records or hold providers accountable.

5.2 The Paradigm Shift: The Nigeria Data Protection Act 2023

The enactment of the Nigeria Data Protection Act (NDPA) 2023 was a watershed moment. Section 34 of the Act reclassifies the patient from a passive subject to an active data subject with enforceable

rights. By defining health data as "sensitive personal data" in section 65, the Act in section 30 imposes stricter processing conditions. Key rights granted to patients (data subjects) under the NDPA include:

a. Right of access *(section 34):* The right to obtain a copy of their personal data in a commonly used electronic format.
b. Right to data portability *(section 38):* A revolutionary right to receive their data in a structured, machine-readable format and transmit it to another provider. This right, inspired by the EU's General Data Protection Regulation (GDPR), has the potential to break down data silos and foster competition and continuity of care.
c. Rights to rectification, erasure, and restriction of processing *(*sections 35, 36, 37*):* Empowering patients to correct inaccuracies and control further processing of their data.

Crucially, section 63 of the NDPA gives it supremacy over any inconsistent provision in prior laws like the NHA 2014, effectively nullifying clauses that denied patient access.

6. The Indian Framework: A Tapestry of Consumer Jurisprudence and Evolving Statute

India's journey has been different, characterized not by a single legislative breakthrough but by a gradual, court-driven evolution towards recognizing patient rights, primarily through the lens of consumer protection.

6.1 Regulatory guidance and judicial activism

Regulation 1.3.2 of the MCI Regulations 2002 mandates that medical records be provided to patients or their authorized attendants within 72 hours of a request. This creates a clear, albeit ethically-based, obligation. Indian courts, particularly the National Consumer Disputes Redressal Commission (NCDRC) and various State Commissions, vigorously enforced this right.[23,24] In a series of landmark judgments, the courts ruled that:

a. Withholding medical records constitutes "deficiency in service" under the Consumer Protection Act.
b. Adverse inferences can be drawn against hospitals that fail to produce records in negligence cases.[25]
c. The defence of "routine destruction" of records is unacceptable when litigation is anticipated.[26,27]

This jurisprudence humanized the law, placing the patient's right to know and seek redress at the forefront.[28]

6.2 The Digital Personal Data Protection Act (DPDPA) 2023

India's new DPDPA 2023, seeks to consolidate this framework into a modern data protection regime. Like Nigeria's NDPA, sections 6, 7, 11 and 12 of the DPDPA requires explicit consent for processing health data, and grants rights of access and erasure. However, it contains some significant drawbacks compared to the NDPA. First, it fails to define health data or categories it as sensitive personal data, although section 7 includes health services as one of the 'legitimate uses' for which data can be processed. This reduces the effectiveness of the Act in protecting health data compared to the NDPA, which imposes a duty on the data controller or data processor to assess the risks involved in handling such sensitive health data. Second, its implementation is still in its infancy,[29] and its interaction with the existing sector-specific rules (MCI Regulations) and powerful consumer jurisprudence remains to be tested. A critical omission, compared to Nigeria's NDPA, is the lack of an explicit right to data portability, which could be a significant drawback for patients in a fragmented healthcare market.[30, 31] Social criticism strengthens legal system by ensuring laws dealing with societal needs for data privacy with enhancing transparency, fostering civic trust, and contributing to a more equitable and sustainable legal system.[32]

7. Comparative Analysis: Two Paths to a Common Goal

The comparison is given in Table 1.

Table 1: Comparative Analysis Nigeria & India.

Feature	Nigeria (Post-NDPA 2023)	India (Post-DPDPA 2023)
Core Legal Basis	Dedicated, comprehensive data protection law (NDPA)	New data protection law (DPDPA) layered over strong consumer protection law and medical ethics regulations.
Right of Access	Statutory right to access and copy.	Statutory right under DPDPA, plus a pre-existing regulatory (MCI) and judicial mandate for access within 72 hours.
Data Portability	Explicit statutory right to receive data in a machine-readable format and transmit it.	Not explicitly provided in the DPDPA (a significant gap).
Enforcement Mechanism	Nigeria Data Protection Commission (NDPC)	Data Protection Board of India (DPBI) – yet to be fully operationalised;[31] currently heavily

		reliant on judicial enforcement.
Historical Context	Radical shift from a restrictive, paternalistic model to a liberal, rights-based one.	Evolutionary development, with courts using consumer law to create a *de facto* rights regime ahead of formal statute.
Biggest Challenge	Implementation and cultural change. Overcoming deep-seated institutional resistance in the healthcare sector and building the capacity of the new NDPC	Integration and clarity. Harmonizing the new DPDPA with existing powerful laws (Consumer Protection Act, MCI rules) and ensuring the new DPBI is effective.

This comparison reveals that Nigeria has, on paper, leaped ahead with a more GDPR-aligned framework, particularly with its inclusion of data portability.[33] India, however, has the advantage of a well-established body of case law that has already normalized the concept of patient data rights for both the public and the judiciary.[34]

8. Conclusion and Recommendations: The Road Ahead for Data Sovereignty

The enactment of the NDPA 2023 signals a commitment to bring Nigeria's data protection standards in line with global norms. India's framework, while currently more complex and lacking in portability, is built on a solid foundation of judicial precedent that has actively protected patients for over two decades. However, for patients in both countries to truly enjoy data rights and protection under the new legal frameworks, Nigeria must implement the newly adopted General Application and Implementation Directive (GAID) 2025, which provides clarity on data portability right, including technical standards, timelines, and permissible fees under the NDPA regime.

The Nigeria Data Protection Commission must also embark on awareness campaigns to educate patients and healthcare providers about their new rights and obligations, and build enforcement capacity to ensure compliance and impose meaningful sanctions for violations. India on the other hand, must provide clear guidance on harmonizing the DPDPA with the Consumer Protection Act 2019 and MCI regulations to avoid legal confusion. It must consider a future amendment to the DPDPA to introduce a right to data portability similar to the position under the NDPA 2023, to further empower patients and promote interoperability in the healthcare sector. The Data Protection Board of India must be set up expeditiously to provide a dedicated and expert enforcement authority. More so, the courts in both countries must continue to play a proactive role in interpreting these new laws in favor of patient autonomy and privacy, and finally, the development of a secure, standardized, and interoperable Electronic Health Record system must be prioritized to make these rights technically feasible.

Contributor ship of Author: All authors equally contributed.

Conflict of interest: None to declare.

Source of funding: None to declare.

References:

1. Basil NN, Ambe S, Ekhator C, Fonkem E. Health Records Database and Inherent Security Concerns: A Review of the Literature. Cureus.2022; 14(10): e30168.
2. Mair J. Who Owns the Information in the Medical Record? Copyright Issues. Health Inf Mgt J. 2011; 40(3):31-7.
3. Hooghiemstra T. Informational Self-Determination, Digital Health and New Features of Data Protection. EDPL.2019; 2: 160.
4. Oke GI, Sibomana O. Adoption of Digital Health Technology in Nigeria: A Scoping Review of Current Trends and Future Directions. Adv Public Health. 2025; 2025(1):4246285.
5. Dahdah MI, Mishra RK. Digital Health for All: The Turn to Digitized Healthcare in India. Soc Sci Med. 2023; 319: 114968.
6. Floyd PT, Oates JC, Acker JW, Warren RW. Defining the Medical Record: Relationships of the Legal Medical Record, The Designated Record Set, and the Electronic Health Record. Perspect Health Inf. Manag. 2021; 18(4): 4.
7. Olukorode SO, Adedeji OJ, Adetokun A, Abioye AI. Impact of Electronic Medical Records on Healthcare Delivery in Nigeria: A Review. PLOS Digit Health. 2024; 3(9): e0000420;
8. Onyegbule KG, Nnaemeka NE. Protecting Patient Confidentiality in Nigeria: Legal, Ethical, and Public Health Perspective. NAU J Comm Prop L.2025; 12(2): 11-2.
9. Medical Council of India (Professional Conduct, Etiquette and Ethics) Regulations, 2002.
10. Deokar RB, Patil SS, Chavan KD. Current Medical Ethical Issues. Int J Educ Res Health Sci 2019; 2(3):1-3.
11. Kerr G, Kulshreshtha N, Greenfield G, Li E, Beaney T, Hayhoe BW et al. Features and frequency of use of electronic health records in primary care across 20

countries: a cross-sectional study. Pub Health. 2024; 233:45-53.
12. Alhomidan ZS, Albaqami NM, Alshehri AA, Aldubaib AA, Alsuwailem AB, Ghadam KFA. Confidentiality in the era of electronic health records: ethical challenges and solutions. Int J Community Med Public Health. 2025; 12(4): 1904–10.
13. Vayena E, Blasimme A. Health research with big data: Time for systemic oversight. J Law Med Ethics. 2018; 46(1): 119–29.
14. Dornan L, Pinyopornpanish K, Jiraporncharoen W, Hashmi A, Dejkriengkraikul N, Angkurawaranon C. Utilisation of Electronic Health Records for Public Health in Asia: A Review of Success Factors and Potential Challenges. BioMed Res Int'l.2019; 8: 7341841.
15. Tahir H, Brezillon P. Data Anonymization Process Challenges and Context. Int'l J Database Mgt Sys.2023; 15(6): 1-10.
16. Adedipe AA, Oke C, Oke B. Enhancing Data Privacy: Pseudonymization and the Nigeria Data Protection Act (2023). Duale, Ovia & Alex – Adedipe Legal Associates, 2024, [cited on 16th Sept 2025]. Available from: https://www.doa-law.com/wp-content/uploads/2024/08/Pseudonymization-Article_v2.pdf
17. Winter JS, Davidson E. Big Data Governance of Personal Health Information and Challenges to Contextual Integrity. The Inf Soc. 2019; 35(1): 36-51.
18. Park HA. The Dt Min Protocol: Implementing Data Minimization Principles in Medical Information Sharing. Electronics. 2025; 14: 1501.
19. Sood A, Mishra D, Surya V, Singh H, Sundaresan R, Pal D et al. Challenges and Recommendations for Enhancing Digital Data Protection in Indian Medical Research and Healthcare Sector. NPJ Digit Med.2025; 8(1):48.
20. Akker van den OR, Stark S, Strech D. Ethics Practices Associated with Reusing Health Data: An Assessment of Patient Registries. BMC Med. 2024; 22: 577.
21. Idoko B, Alakwe JA, Ugwu O, Idoko JE, Idoko FO, Ayoola VB et al. Enhancing healthcare data privacy and security: A comparative study of regulations and best practices in the US and Nigeria. Magna Scientia Adv Res Reviews. 2024; 11(2): 151-67.
22. Aderibigbe TO, Sodipo B. Patient's Medical Records, Privacy and Copyright in Nigeria: On-going Research. Univ Western Austr L Rev.2017; 42(2): 89-90.
23. Athavale SU. Digi Doctor- Concise Review of Telemedicine Practice Guidelines, 2020. J Forensic Med Sci Law. 2021; 30(2):63-6.
24. Gupta M, Gupta, B. Consumer Protection Act in Medical Practice: A Narrative Review from an Indian Perspective. Int J Med Pub Health. 2025; 15(3): 1981-7.
25. Kanaiyalal Ramanlal Trivedi v Dr. Satyanarayan Vishwakarma (1996) 3 CPR 24 (Guj); (1997) 1 CPJ 332 (Guj); (1998) CCJ 690 (Guj). Ozair Husain v Union of India, AIR 2003 Delhi 103.
26. Patil SS, Deokar RB, Dere RC. Euthanasia and Living Will -Right to Die with Dignity: A Literature Review. J Forensic Med Sci Law. 2023; 32(2):75-9.
27. Dr. Shyam Kumar v Rameshbhai, Harmanbhai Kachiya (2002) 1 CPR 320; (2006) 1 CPJ 16 (NC).
28. Deokar RB, Patil SS. Cybercrime: Medicolegal Perspective. J Forensic Med Sci Law. 2025;34(1):1-3. doi: 10.59988/jfmsl.vol.34issue1.1
29. SA Quereshi v Padode Memorial Hospital and Research Centre II (2000) CPJ 463 (Bhopal).
30. Deokar RB, Patil SS. Artificial Intelligence in Healthcare and Biomedical Research - Ethical aspects. J Forensic Med Sci Law. 2024;33(1):1-4. doi: 10.59988/jfmsl.vol.33issue1.1
31. Bahl R, Bagai R, Ghoshal S, Iyer A. Data Protection Laws and Regulations India 2025. International Comparative Legal Guides, 2025, [cited on 24th Sept 2025]. Available from: https://iclg.com/practice-areas/data-protection-laws-and-regulations/india
32. Bich NN, Tuan VV. Social Criticism and its Impact on Law-Making Activities in Vietnam: A Critical Analysis. J Forensic Med Sci Law. 2025;34(1):44-49. doi: 10.59988/jfmsl.vol.34issue1.9
33. Centre for Health Equity, Law & Policy, Endangering Health Data: An Issue Brief on India's Data Protection Law, Indian Law Society 2024, [cited on 26th Sept 2025]. Available from: https://bfda9b73-bb63-4945-b64d-2477e3eb985d.usrfiles.com/ugd/bfda9b_2a1937feefe84d0b9b0847802d2493a1.pdf
34. N Viswanath, G Kedia. 'Operationalising the DPDPA: Implementing Consent Management Systems', Mondaq, 20 June 2025, [cited on 30th Sept 2025]. Available from: https://www.mondaq.com/india/privacy-protection/1639922/operationalising-the-dpdpa-implementing-consent-management-systems.