PATIENTS' RIGHT TO DATA PRIVACY AND PROTECTION IN NIGERIA: A RIGHT OR PRIVILEGE?

[1]Eyiuche Stella AHANWA, PhD
[2]Nkechi Elizabeth OFFORMA, PhD
[1] Private and Property Law Department, Faculty of Law,
Nnamdi Azikiwe University, Awka, Anambra.
[2] Faculty of Law, Abia State University, Uturu, Abia State.
[1] es.ahanwa@unizik.edu.ng
[2] elizofforma@gmail.com

Abstract

The digital transformation of healthcare has intensified concerns surrounding the protection of patient health data globally. In Nigeria, the question of whether data privacy constitutes a fundamental right or a mere privilege for patients remains largely unresolved, creating significant gaps in legal protection and clinical accountability. This study adopts a doctrinal methodology and a comparative approach. This research examines the legal framework governing patient data privacy in Nigeria, with particular focus on the Nigeria Data Protection Act 2023, the National Health Act 2014 and other relevant laws. It further interrogates the extent to which these instruments adequately protect patient health information and analyses the tensions between regulatory intent and practical enforcement. Drawing on comparative analysis with the United Kingdom's General Data Protection Regulation (GDPR), it is argued that patient data privacy in Nigeria is constitutionally grounded and must be treated as a fundamental right, not a discretionary privilege. It further identifies systemic enforcement failures, institutional non-compliance, and low patient awareness as critical barriers to realising this right. The article concludes by recommending legislative harmonisation, stronger regulatory oversight, and mandatory data protection compliance frameworks tailored specifically to the Nigerian healthcare sector.

Keywords: Data privacy, Healthcare, Health personnel, National Health Act, Patient rights.

1. Introduction

Patients disclose a lot of sensitive medical information whenever they go to health facilities to access healthcare. When documented, the information given out by the patients become patients' records. Over the years, global efforts have been made legislatively to guide health personnel in handling patients' information during healthcare delivery.[685] While some countries have unique laws specifically made to regulate data privacy during medical consultations, others do not. Japan, Australia, USA and Spain have specific laws regulating privacy of patients' information.[686] Other countries like Nigeria, South African and several other do not have specific laws regulating the privacy of information shared by patients during medical consultations. Nigeria, for example has several laws regulating the management of patients' data that include the National Health Act. 2014 and the Nigeria Data Privacy Act, 2023.

The present research is primarily focused on reviewing the laws protecting the privacy of information shared by patients during medical consultations in Nigeria. The first attempt is seen in the provision of the Constitution of the Federal Republic of Nigeria that guaranteed the right to privacy generally with exceptions. Then there is the National Health Act that obligates health professionals to preserve the confidentiality of information shared by patients and also the need to restrict access to patients' information also, with recognized exceptions. The Nigeria Data Protection Act provides principles to be adhered to by health professionals while handling patients' personal information. A good number of regulatory bodies with roles to play in the proper handling of patient data with requisite privacy are also looked at in this research such as the Courts and the Nigeria Data Protection Commission. Problems hampering strict privacy of patients' data are identified and include health professionals' ignorance of the provisions of the laws regulating the collection and processing of patients' data and also inadequately trained persons handling patients' medical information in private hospitals.

To make the research more meaningful, the legal landscape in the UK for the regulation of the privacy of patients' data gotten in the course of medical consultations was also examined. The aim

[685] WHO, 'The protection of personal data in health information systems – principles and processes for public health.' https://iris.who.int/server/api/core/bitstreams/2f9bfa5b-4fcd-4553-a211-6ea19686ea4d/content retrieved on April 27, 2026.
[686] World Bank, 'Data Protection and Privacy Laws' https://id4d.worldbank.org/guide/data-protection-and-privacy-laws retrieved on April 27, 2026.

was to appraise the UK legal system for lessons that can improve what we have in Nigeria. The methodology adopted in the present research is doctrinal, analytical, and comparative.

2. Conceptual Foundations: Data Privacy as a Human Right

2.1. The Nature of Privacy as a Right

Privacy, in its broadest sense, is the individual's claim to control information about themselves – to determine what is known, by whom, and for what purpose.[687] As Warren and Brandeis articulated in their seminal 1890 Harvard Law Review essay, privacy is fundamentally the "right to be let alone." While that formulation emerged in a pre-digital era, it retains remarkable resonance in contemporary debates about informational autonomy.[688] At the international level, the right to privacy is firmly anchored in human rights law. Article 12 of the Universal Declaration of Human Rights 1948 prohibits arbitrary interference with a person's privacy. Article 17 of the International Covenant on Civil and Political Rights (ICCPR), to which Nigeria is a signatory, reinforces this protection by requiring states to provide legal safeguards against such interference. The United Nations General Assembly Resolution 68/167 of 2013 further affirmed that the right to privacy extends fully to the digital environment.[689]

Health data occupies a uniquely sensitive position within the broader category of personal data.[690] It touches on the most intimate dimensions of human existence — physical vulnerability, mental condition, reproductive choices, genetic identity, and mortality. The exposure of such information without consent can cause profound harm: discrimination in employment and insurance, social stigma, damaged relationships, psychological injury, and loss of autonomy over one's own narrative. For these reasons, health data has consistently been treated as a special category deserving heightened protection across international and comparative legal frameworks.

[687] A Lukacs, 'What is Privacy: The History and Definition of Privacy.' https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf retrieved on April 27, 2026.
[688] *Ibid.*
[689] *Ibid.*
[690] N Liu and S Chen, 'The Protection Mechanism of Personal Health Information in the Digital Economy Environment.' (2022) Jounal of Environmental and Public Health, https://pmc.ncbi.nlm.nih.gov/articles/PMC9208985/ retrieved on April 27, 2026.

2.2 The Right-Privilege Distinction in Legal Theory

The distinction between a right and a privilege is foundational to legal theory and has direct bearing on this paper's central inquiry. A right, imposes a correlative duty on another party.[691] If a patient has a right to data privacy, then healthcare providers, institutions, and the state bear a corresponding duty to protect that privacy. Breach of that duty gives rise to legal liability and remedial action.

A privilege, by contrast, is a benefit conferred at the discretion of another.[692] It may be withdrawn, conditioned, or withheld without legal consequence. If patient data privacy were merely a privilege in the Nigerian legal context, it would mean that protection depends entirely on the voluntary choices of healthcare providers a proposition that is both legally untenable and morally indefensible.

The position taken in this paper is that patient data privacy is not, and cannot properly be characterised as, a privilege. It is a right that is grounded in constitutional provisions, statutory protections, and Nigeria's international human rights obligations. The problem is not one of legal existence but of legal enforcement.

3. Legal Issues in the Management of Patients' Medical Records by Health Institutions and Health Personnel

The primary purpose of medical records is to document the course of patients' health care and provide a means of health communication among health care professionals for current and future use.[693] During medical consultations, health personnel are involved in getting sensitive information from patients and the individual information gotten from patients all together form the general medical records of health institutions. The process of garnering data from patients has legal implications and issues arising thereby. Some of the major issues arising from health personnel's collection, processing and storage of patients' data in health institutions' data base are briefly examined below.

[691] K Gupta, 'Theories of rights: an overview of Hohfeld's analysis of rights.' https://blog.ipleaders.in/theories-of-rights-an-overview-of-hohfelds-analysis-of-rights/ retrieved on April 27, 2026.
[692] GK Today, 'Privilege and a Right.' https://www.gktoday.in/privilege-and-a-right/ retrieved on April 27, 2026.
[693] I T Adeleke, *et al,* 'Knowledge, Attitudes and Practice of Confidentiality of Patients' Health Records among Health Care Professionals at Federal Medical Centre, Bida.' (2011) Nigerian Journal of Medicine, p 229.

3.1. Access to Patients' Medical Records: Rights, Limits, and Authorized Persons

As a general rule, a patient's medical record is a confidential document with restricted access to it.[694] Globally, patients' right to access their medical records in any health institution where such health records exist is recognized. Canada, Brazil and Australia are part of a good number of countries that recognize this right.[695] Chile is part of those other few countries that do not allow patients access their medical records freely.

Professionally, health care providers are ethically and legally required to maintain patient treatment records.[696] This is so because patients' treatment records form part of a health institution's general medical record. Although patient medical records are regulated by patient welfare-oriented healthcare principles, the record is also a legal document. It serves to protect the legal interests of all participants in the health care delivery system worldwide.

It may appear that amongst themselves, health personnel within a health institution generally have access to patients' data in their medical records. Legally and ethically speaking, it is only health workers directly working on a patient that can have access to such patient's medical records.[697]

In Nigeria, the right of access to a patient's medical record is not expressly recognized and guaranteed but a proper reading the provisions of sections 26 – 29 of the National Health Act suggest that users of healthcare facilities may be allowed access to their medical record upon request. Access to health records also pertains to third party access to a patient's medical records consequently affecting their access also.

3.2. Confidentiality and Privacy

The right to privacy has a relationship with human dignity and personal autonomy as it derives from the right to be let alone. The privacy of a patient's health information is a pertinent part of healthcare services related to the management of individual health data.[698] Patient privacy as regards data protection connotes the patient's right to the security and confidentiality of their health

[694] H Rosenmann, 'Patients' Rights to Access their Medical Records: An Argument for Uniform Recognition of a Right of Access in the United States and Australia.' (1997) Fordham International Law Journal, 1505.
[695] S Howard, 'Patients' Access to Medical Records around the World.' (2024) BMJ, https://www.bmj.com/content/386/bmj.q1481.full retrieved on February 20, 2026.
[696] H Rosenmann, *op. cit.* p. 1506.
[697] These are seen in the provisions of the National Health Act.
[698] W Rahayu, 'Legal Framework or Health Data Protection: Balancing Patient Privacy and Institutional Needs.' (2025) International Journal of Health Administration Law and Government Policies, 36.

information, which includes diagnosis, medical history, treatment, and other sensitive data. Protecting patient privacy has ethical and legal implications which makes it regulated by several policies and laws, in order to create a safe and comfortable environment for patients to share information with healthcare providers.

Amongst health personnel, the insistence that health related information should be kept private, is a key element of ensuring that the trust reposed on the health personnel by the patient by sharing sensitive information is not breached.[699] The contents of medical record must be kept confidential to protect patient confidentiality. Hospitals must protect the physical record of medical record as archives. Overall, patient privacy and health data protection are important pillars in providing quality health services.[700] Protecting patient privacy means respecting individual dignity and rights, as well as creating a climate in which patients feel safe to share the information needed to improve their health. This not only benefits patients but also supports healthcare providers in providing better and more targeted care.

Globally and domestically, there are various legal instruments that guide the protection and privacy of patients whilst ensuring that within permitted exceptions, patients' medical history divulged during medical consultations are kept confidential. These legal instruments are examined subsequently.

3.3. Consent to the Collection, Use, and Disclosure of Patients' Data

Informed consent is a key ethical/medico-legal principle that must be observed during medical consultations between patients and health personnel. In rendering healthcare services/products to patients or even getting information from patients, medical personnel are obligated to seek and get consent. Informed consent goes beyond signing documents – it is a communication process between the health personnel and the patient.[701] This process ensures that the patient is fully informed about the nature of the procedure or intervention, the potential risks and benefits, and the

[699]World Health Organization, "Legal Frameworks for e-Health.' https://iris.who.int/bitstream/handle/10665/44807/9789241503143_eng.pdf?sequence=1&isAllowed=y#:~:text=In%20the%20practice%20of%20the,or%20sharing%20health%20related%20information. retrieved on February 20, 2026.
[700] W Rahayu, *op. cit.*, 37.
[701]P Shah, *et al,* 'Informed Consent.' https://www.ncbi.nlm.nih.gov/books/NBK430827/?report=reader#_NBK430827_pubdet_ retrieved on February 20, 2026.

alternative treatments available. The patient can refuse or withdraw consent at any time during treatment. Informed consent respects patient autonomy, promotes trust in the patient-provider relationship, and safeguards against unethical practices.[702] Legally speaking, whatever medical treatment is to be administered to a patient, the patient's consent is paramount irrespective of how trivial the treatment or therapy seems.[703]

4. Legal Landscape for the Regulation of Patients' Data Privacy and Protection in Nigeria

Presently in Nigeria, there exist various laws that control the retrieval and handling of the data gotten from patients during medical consultations. There are also several administrative bodies involved in the handling of patients' information. Some of the said laws and administrative bodies are examined below.

4.1. Statutory Regulation of Patients' Data Privacy in Nigeria

In Nigeria, the Constitution of the Federal Republic of Nigeria, the Nigeria Data Protection Act and some other laws regulate patients' data. They are discussed hereunder.

4.1.1. Health Records Officers (Registration, Etc.) Act, 1989.

The Health Records Officers (Registration Board of Nigeria etc.) Act establishes the Health Records Officers Registration Board of Nigeria which interestingly make the management of health records a professional affair with ethics and rules for managing the data of patients in Nigeria.[704] The Board regulates the training of health records officers or managers. These health records managers are actually health care professionals, responsible for collecting, capturing, storing, analyzing distributing and protecting medical information, fundamental to providing quality patient care.[705] The data handled by these cadre of health professionals is what medical doctors and several other health personnel work with in managing patient care in healthcare delivery.

[702] *Ibid.*
[703] Y Omlomojobi, 'Right to Privacy.' https://ssrn.com/abstract=3062603 retrieved on February 20, 2026.
[704]Health Officers (Reg.) Act, section 1.
[705] S. M. Omole A. O. Ogunniran T. T. Adebayo, 'Professionalism and Health Records Management Practice in Nigeria.' (2018) International Journal of Finance and Management in Practice, p. 18.

4.1.2. The Constitution of the Federal Republic of Nigeria, 1999, (as amended).

The Constitution of the Federal Republic of Nigeria[706] specifically recognizes the right to privacy as follows: the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.

It accords with common sense to assert that the above provision protects personal information disclosed by patients in the course of physical and virtual medical consultations. By necessary implication, health professionals have a duty to respect and protect the privacy of data disclosed by patients.

Section 45 (1) of the CFRN lucidly points out that the right to privacy in Nigeria is not absolute and can be breached:

> (a) in the interest of defence, public safety, public order, public morality or public health; or
>
> (b) for the purpose of protecting the rights and freedom of other persons.

Epidemics and pandemics fall under circumstances that the right of privacy will be breached in protection of the general public. In fact, during the Coronavirus pandemic, the identity of a foreigner who had the virus was made public to make it easier to traces persons that came in contact with him in order to quarantine and treat infected person.[707]

4.1.3. National Health Act, 2014.

The National Health Act[708] generally regulates healthcare delivery in Nigeria. Specifically, section 25 of the NHA provides that every person in charge of a health establishment shall ensure that a health record containing such information as may be prescribed is created and available at that health establishment for every user of health services. By necessary implication, health establishments are obligated to collate and preserve patients' health information in the professionally prescribed manner and such health information should be accessible by such patients. The mode of collecting and storing date is not expressly provided for in section 25 but

[706] Hereinafter referred to as CFRN, section 37.
[707] Nigeria Centre for Disease Control, 'First Case of Corona Virus Disease Confirmed in Nigeria.' https://ncdc.gov.ng/news/227/first-case-of-corona-virus-disease-confirmed-in-nigeria retrieved on February 2, 2026.
[708] Hereinafter referred to as the NHA.

when the said provision of the NHA is read reading the said provisions with the laws like the Health Records Officers (Registration, etc) Act raise the presumption that collation and preservation of medical records should be in accordance with the ethics of health records officers and suchlike.

Additionally, the NHA, clearly states that all the information pertaining to a patient, which also incorporates information relating to such patient's health status, treatment or stay in a health establishment shall be kept confidential.[709] In section 26 (2) provision is made for exceptional circumstances, subject to section 27, where a patient's data may be disclosed which include –

1. When the patient consents to disclosure in writing;
2. a court order or any law requires that disclosure;
3. in the case of a minor, with the request of a parent or guardian;
4. in the case of a person who is otherwise unable to grant consent upon the request of a guardian or representative; or
5. non-disclosure of the information represents a serious threat to public health.

The foregoing clearly put in place a general rule: that health workers are obligated to keep patients' information confidential but this is subject to stated exceptions listed therein.

In the course of carrying their official duties and in the interest of a patient, health workers that have access to a patient's health record are allowed to disclose such patient's personal data to any other person, health care provider or health establishment as is necessary for any legitimate purpose within the ordinary course and scope of his or her duties.[710] This section can reasonably be said to come within the exception to keep a patient's medical records confidential. In the interest of the patient, section 27 allows health personnel to disclose details of the patient's medical records.

A health care provider may examine a patient's health records for the purpose of:

a. treatment with the authorization of the patient; and

[709] NHA, section 26 (1).
[710] NHA, section 27.

b. study, teaching or research with the authorization of the user, head of the health establishment concerned and the relevant health research ethics committee. [711]

Where a patient's identity is not reflected in such study described above, authorization would not be necessary.[712]

Persons in charge of health establishments who are in possession of patients' health records are mandated to set up control measures to prevent unauthorized access to patients' records and to preserve the storage facilities in which, or systems by which, records are kept.[713] It could reasonably be said that this is in the line of duties of health records officers discussed earlier.

The NHA provides offences and punishments for non-compliance with the sections of the NHA on management of patients' records.[714]

4.1.4. The HIV and AIDS (Anti-Discrimination) Act, 2014

The HIV and AIDS (Anti-Discrimination) Act[715]obligates health establishments to respect the privacy rights of individuals afflicted with HIV/AIDS. It is safe to make this assertion when the HAAD Act is read in consonance with the right to privacy in the CFRN.

By the provisions of section 13 (1) of the HAAD Act the right to protection of data of persons living with and affected by HIV/AIDS with respect to their health and medical records. Non-compliance with the provisions of section 13 (1) is punishable, upon conviction, with a fine not less than #500,000 for individuals and not less than #1,000,000 for institutions; or imprisonment not exceeding 2 years or both**.**

4.1.5.Nigeria Data Protection Act, 2023

The Nigeria Data Protection Act[716] was enacted to provide a legal foundation for the protection of personal information, and establish the Nigeria Data Protection Commission for the regulation of the processing of personal information.[717]

[711] NHA, section 28 (1)
[712] NHA, section 28 (2).
[713] *Ibid.* section 29 (1).
[714] NHA, section 29.
[715] Hereinafter referred to as HAAD Act.
[716] Hereinafter referred to as the NDPA.
[717] See the long title of NDPA.

Section 4 of the NDPA establishes the Nigeria Data Protection Commission[718] and it has several functions[719] that revolve around the implementation of the NDPA.[720]

Outlined in the NDP Act are the principles and lawful basis governing processing of personal data in Nigeria.[721] During medical consultations, health professionals garner a lot of personal information from patients. The said principles in the NDPA[722] on processing personal data apply to health professionals as they get a lot of sensitive personal information from patients during medical consultations.

For instance, such data should be:[723]

1. processed in a fair, lawful and transparent manner;
2. collected for specified, explicit, and legitimate purposes, and not to be further processed in a way incompatible with these purposes;
3. adequate, relevant, and limited to the minimum necessary for the purposes for which the personal data was collected or further processed;
4. accurate, complete, not misleading, and, where necessary, kept up to date having regard to the purposes for which the personal data is collected or is further processed; and
5. processed in a manner that ensures appropriate security of personal data, including protection against unauthorized or unlawful processing, access, loss, destruction, damage, or any form of data breach.

The NDPA provides several rights of a data subject enjoys as regards the garnering, handling and storage of the data subject's personal data. Such rights include –[724]

1. right of the data subject to withdraw consent, at any time, consent to the processing of personal data under the NDPA.
2. right to a copy of data subject's personal data in a commonly used electronic format except to the extent that providing such data would impose unreasonable costs on the data

[718] NDPA, section 4 (1)
[719] NDPA, section 5.
[720] *Ibid.* section 6 (a).
[721] NDPA, part 5: sections 24 – 33.
[722] *Ibid.*
[723] *Ibid.,* section 24 (1) (a) – (f).
[724] NDPA, part 6 generally.

controller, in which case the data subject may be required by the data controller to bear some or all of such costs.

3. Right to withdraw, at any time, consent to the processing of personal data under the NDPA.

These rights contained in the NDPA align with the patient's rights in other statutes such as the NHA and the Constitution.

Again, an appraisal of the NDPA shows that it generally protects the rights of a patient during medical consultations and also the handling of patients' medical records. The real issue that remains is whether health personnel are aware of their duties and obligations under the NDPA.

5. Institutional Regulation of Patients' Data Privacy in Nigeria

5.1. The Courts

In Nigeria, one of the major means through which patients can get their right to privacy protected and enforced is through the courts. By the provisions of section 6 (6) (b) of the CFRN courts hear suits for the enforcement of rights of persons in Nigeria as follows:

The judicial powers vested in accordance with the foregoing provisions of this section –

> (b) shall extend to all matters between persons, or between government or authority and to any person in Nigeria, and to all actions and proceedings relating thereto, for the determination of any question as to the civil rights and obligations of that person;

The CFRN recognized the right to privacy, hence, a patient whose right to privacy is about be breached or has been breached can seek redress through civil action to enforce/protect their right to privacy. The researchers of this paper, at the time writing the paper did not come across any reported case pertaining to the breach of a patient's right to privacy.

5.2. The Ministries of Health

By the combined reading of sections 1, 2 and 3 of the NHA, the Federal Ministry of Health and States Ministry of Health have an administrative role in the implementation of the provisions of the National Health Act by public and private health establishments. By necessary implication, the Federal and State Ministries of Health have administrative control over health establishments and can sanction those of them that are not in compliance with the provisions of the NHA. Hence, health establishments that do not comply with the provisions of the NHA that touch on access to

the health records of patients can be called to order or sanctioned through the relevant Ministry of Health.

5.3. Regulatory Bodies of the various Health Professionals

Various health professionals have their regulatory bodies that regulate their professional conduct. For medical doctors and dentists, the Medical and Dental Council of Nigeria regulate them professionally.[725] They have quasi-judicial bodies through which they investigate and try practitioners against whom complaints of professional misconduct have been reported: the Medical and Dental Practitioners' Investigation Panel and the Medical and Dental Practitioners Disciplinary Tribunal. The digitally, complaints against doctors and dentists can channeled to the Medical and Dental Council of Nigeria through its website: https://www.mdcn.gov.ng/.

5.4.The Nigerian Data Protection Commission

By the provisions of section 4 of the NDP Act, provision is made for the Nigeria Data Protection Commission and it is tasked with diverse functions that include to –

1. regulate the deployment of technological and organizational measures to enhance personal data protection;
2. promote awareness on the obligation of data controllers and data processors under the NDPA
3. promote public awareness and understanding of personal data protection, rights and obligations imposed under the NDPA, and the risks to personal data;
4. receive complaints relating to violations of the NDPA or subsidiary legislation made under the NDPA
5. collect and publish information with respect to personal data protection, including personal data breaches;
6. advise government on policy issues relating to data protection and privacy

Additionally, section 6 of the NDPA, the NDPC has several powers that include the investigation of data controllers/data processors violation of the provisions of the NDPA or subsidiary legislation made under the NDPA; overseeing the implementation of the NDPA; and imposition of

[725] MDCN, 'Disciplinary Tribunal.' https://www.mdcnigeria.org/mdcn-disciplinary-tribunal/#:~:text=Medical%20and%20Dental%20Practitioners%20Disciplinary,liable%20to%20appropriate%20disciplinary%20action.retrieved on February 15, 2026.

penalties in respect of any violation of the provisions of the NDPA or subsidiary legislation made under it.

Pursuant to the powers and functions vested on the NDPC, where it finds a data processor or data collector liable for violating the provisions of the NDPA, the NDPC can make compliance orders against such violators. It is pertinent to mention that when the NDPC makes orders of the nature, the said orders which must be in writing include [726]

(a) a warning that certain act or omission is likely to be a violation of one or more provisions under the NDPA or any subsidiary legislation or orders issued under it;

(b) requiring that the data controller or data processor acts in accordance with such provisions, in addition to compliance with the requests of a data subject to exercise one or more rights under the NDPA; or

(c) 'cease and desist order' that requires such data controller or data processor to stop or refrain from doing an act, which is in violation of the NDPA, including stopping or refraining from processing personal data that is the subject of the order.

The NDPC can also make enforcement orders in relevant circumstances.[727]

With the powers vested on the NDPC and the provisions of the NDPA, the NDPC is empowered to enforce diverse rights of patients recognized by the NDPA and also the provisions of the NDPA against erring health personnel who breach data privacy principles in handling patients' personal information.

6. Legal Regulation of Patients' Data Privacy and Protection in the UK Health Sector

In the UK, patients generally have access to their personal health records but restricted access to that of other persons.[728] In exceptional circumstances, a patient may be denied access to his or her health record: where it would likely cause harm.

With respect to patient privacy, a good number of laws regulate it in the UK. The General Data Protection Regulation made pursuant to the Data Protection Act of 2018 regulates access to

[726] See NDPA, section 47 generally.
[727] See section 48 generally.
[728]House of Commons Library, 'Patient health records: Access, sharing and confidentiality.' https://commonslibrary.parliament.uk/research-briefings/sn07103/ retrieved February 13, 2026.

patients' records.[729] Where a patient is dead, such patient's health record is accessed in accordance with the Access to Health Records Act of 1990.[730] By the provisions of the AHR Act, access a deceased person's health records can only be granted to a person if they are either:

1. a personal representative (the executor or administrator of the deceased person's estate);
2. someone who has a claim resulting from the death (this could be a relative or another person).

Access to a deceased person's health records may be denied if the patient requested confidentiality whilst they were alive.[731] No information can be revealed if the patient requested non-disclosure. Disclosure may also not take place if there is a risk of serious harm to an individual, or if records contain information relating to another person.

The General Medical Council sets out the circumstances in which information from a deceased person's health records should be disclosed: the duty of confidentiality continues after a patient has died. There are circumstances in which relevant information about a patient who has died must be disclosed –

1. when disclosure is required by law
2. to help a coroner, procurator fiscal or other similar officer with an inquest or fatal accident inquiry
3. on death certificates, which you must complete honestly and fully
4. when a person has a right of access to records under the Access to Health Records Act, 1990 or the Access to Health Records (Northern Ireland) Order, 1993, unless an exemption applies
5. when disclosure is necessary to meet a statutory duty of candour.

In other circumstances, whether and what personal information may be disclosed after a patient's death will depend on the facts of the case. If the patient had asked for information to remain confidential, health personnel should usually abide by their wishes.

[729] A Kulakiewicz and T Powell, 'Patient health records: Access, sharing and confidentiality.' Press Briefing presented to the House of Commons on the 8th of July, 2022.
[730] Hereinafter referred to as AHR Act.
[731] Access to Health Records Act 1990, section 4(3).

Where unaware of any instructions from the patient, when considering requests for information, health personnel should take into account:

1. whether disclosing information is likely to cause distress to, or be of benefit to, the patient's partner or family
2. whether the disclosure will also disclose information about the patient's family or anyone else
3. whether the information is already public knowledge or can be anonymized or de-identified
4. the purpose of the disclosure.

Circumstances in which health personnel should usually disclose relevant information about a patient who has died include:

1. the disclosure is permitted or has been approved under a statutory process that sets aside the common law duty of confidentiality, unless the patient has objected
2. when disclosure is justified in the public interest to protect others from a risk of death or serious harm.

There are certain circumstances in which full access to a patient's health record may be denied.[732] These include cases where the release is likely to cause serious harm to the physical or mental health of the subject or another individual. Prior to release, the data controller should consult with either:[733]

1. The health professional responsible for the individual;
2. Where there is more than one such health professional, the most suitable professional;
3. Where no such professional is available, one with the experience and qualifications to advise accordingly.

Where records disclose information related to another individual, the data controller is not obliged to release the information, except in the following circumstances:[734]

1. The third party is a health professional who has compiled or contributed to the health records or who has been involved in the care of the patient;

[732] A Kulakiewicz and T Powell, *op. cit.*
[733] The Data Protection (Subject Access Modification) (Health) Order 2000, SI 2000/413.
[734] *Ibid.*

2. The third party, who is not a health professional, gives their consent to the disclosure of that information;
3. It is reasonable to disclose without that third party's consent

The Health and Social Care (Safety and Quality) Act, 2015 introduced a legal duty for health and social care professionals to share patient information where they consider disclosure is likely to facilitate patient care and is in the patient's best interest.

The Health and Care Act, 2022 includes measures relating to the collection and sharing of health and care data. These provisions are intended to enable increased sharing and more effective use of data across the health and adult social care system. Specifically, the legislation aims to enable the Department of Health and Social Care and National Health Service, England to publish mandatory information standards to ensure providers of health and adult social care adopt a standardized approach to the collection and processing of data. These provisions extend the potential application of information standards to include private providers of health and adult social care.

There are certain circumstances in which a health professional is required by law to disclose medical information, regardless of a patient's consent.[735] For example, statutory disclosures are required under the following legislation, although this is not an exhaustive list:

1. Health Protection (Notification) Regulations 2010 – a health professional must notify local authorities about any person suspected of having a range of listed conditions, including food poisoning, measles and tetanus.
2. Abortion Regulations 1991 – a doctor carrying out a termination of pregnancy must notify the Chief Medical Officer, giving the individual's date of birth and postcode.
3. Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 – deaths, major injuries and accidents resulting in three days off work, as well as certain diseases and dangerous occurrences, must be reported.
4. Female Genital Mutilation Act 2003 – medical professionals must inform the chief police officer for the area where they learn of, or suspect, female genital mutilation of a girl below 18 years.

[735]A Kulakiewicz and T Powell, *op. cit.*

The British Medical Association provides additional information on legal and statutory disclosures. Some statutes allow, rather than mandate, disclosure of confidential information. For example, under the Children Act 1989, disclosure is permitted to other organizations such as the police or social services if there is a suspicion that a child is suffering, or is at risk of suffering, significant harm. Under section 261 of the Health and Social Care Act 2012, NHS Digital is permitted to disclose information in certain circumstances, including in connection with the investigation of a criminal offence. In contrast, some statutes require health professionals to restrict disclosure of certain confidential information. For example, under the Gender Recognition Act 2004, it is an offence to disclose protected information such as a person's gender history after that person has changed gender. Patient confidentiality can be overridden under section 251 of the NHS Act 2006, which allows for the Secretary of State to set aside the duty of confidentiality for the purposes of research, audit and other medical purposes not directly related to a patient's care.

There are exceptional circumstances in which a health or social care professional may be obliged to share confidential patient information in line with the "public interest." The BMA describes this type of mandatory disclosure as: A disclosure of confidential information because it is in the 'public interest' can be justified if it is essential to:[736]

1. prevent, detect or prosecute serious crime;
2. prevent a serious threat to public health or national security;
3. or to protect individuals or society from serious harm.

Informed consent from the individual must always be sought first, but an individual's right to confidentiality can be overruled to protect the public interest.[737]

NHS Digital also provides guidance on sharing genetic information with family members, where the diagnosis of a condition in the patient might point to the likelihood of the same condition in a blood relative. In circumstances where a patient refuses to give consent to share information, disclosure might still be justified in the public interest. It recommends: If a patient refuses consent to disclosure, health and care staff will need to balance their duty to make the care of the patient their first concern against their duty to help protect the other person from serious harm. If

[736] BMA, Confidentiality and health records toolkit, p14.
[737] HSCIC, A guide to confidentiality in health and social care, September 2013.

practicable, health and care staff should not disclose the patient's identity in contacting and advising others of the risks they face.[738]

Presently, the Data (Use and Access) Act, 2025 was enacted to ensure that information standards can apply to IT providers, IT services, or information processing services used in health or adult social care in England. The government has said that this could address challenges around NHS data being fragmented by giving staff quicker access to it and reducing duplication of lab tests and data entries.

In the UK there are various bodies involved in regulating access to patients' health information. A good number of them have been mentioned earlier and their roles. They include the Department of Health and Social Care, the National Health Service, the British Medical Association, and National Health Service Digital. They all work hand in hand to ensure seamless healthcare delivery.

7. Hindrances in the handling of Patients' Medical Records in Nigeria

Adequate handling and storage of patients' information, research reveals, is a major challenge in Nigeria which caused by diverse factors.[739] A good number of the factors are discussed hereunder.

7.1. Limited Qualified Personnel in the Proper Handling of Patients' Data: Research reveal the existence of a professional Body in Nigeria established for the professional handling of patients' medal information – health record officers. The scanty presence of these officers is seen in mainly government run hospitals while they are absent in privately run health facilities. The down side of this is that the ethics and expertise required in handling patients' data are dispensed with. The sad outcome is that patients' medical records would not be accessible.

7.2. Ignorance on the Position of the Law on the Management of Patients' Records in Health Establishments. In healthcare delivery in Nigeria, how health personnel handle patients' information reveals their ignorance of the legal implication of collecting, processing, storing and managing patients' information. Very common on social media in recent times are pictures and videos posted by health professionals of patients in vulnerable conditions being recorded without their consent. This reveals health professionals' ignorance of the provisions of the NDPA which

[738] *Ibid.,* section 8.
[739] J A Yaya *et al*, 'Challenges of Record Management in two Health Institutions in Lagos State, Nigeria.' (2015) International Journal of Research in Humanities and Social Studies, p. 3.

outlines several principles that should guide health personnel in the management of patients' sensitive information garnered during medical consultations.

7.3. Lack of Regular Training of Health Personnel in the Handling of Patients' Health Records. The researcher herein earlier pointed out the ignorance of some health personnel in handling patients' data**.** It has been observed that this ignorance of the law is a recurring decimal which is a pointer to the fact that health personnel are not regularly trained on the legal handling of patients' data to prevent data breaches.

7.4. Inadequate Infrastructure. This is another challenge that affects proper management of patients' medical records in health facilities. Health personnel have complained about not being properly equipped with infrastructural and technological means to properly manage patients' data at their disposal. Research reveals that a lot of privately owned health establishments still rely on manual/paper storage of patients' data as against digital collection, processing and storage (electronic health records system). Even when health personnel have access to computers and other storage devices, they still lament that epileptic power supply hamper their effectiveness in managing patients' data.

8. Conclusion and Recommendations

The United Nations' third Sustainable Development Goal is access to good health and wellbeing. One of the ways this can happen is when health personnel intentionally ensure the preservation and protection of patients' data privacy during healthcare delivery. In the course of the present research, the researcher highlighted legal issues that come up as a patient accesses healthcare delivery in Nigerian health facilities. Such legal concerns include access to patients' medical records, informed consent, confidentiality and data privacy. Also, the legal framework regulating patients' privacy in the healthcare sectors in Nigeria and UK were also looked at for lessons that can improve the Nigerian landscape. Several challenges hampering the effective protection and privacy of patients' data in healthcare in Nigeria were also identified. In examining the legal framework for the protection of patients' privacy in healthcare, the present researcher discovered that for a start, there are good laws that recognize the privacy a patient should enjoy in accessing healthcare. Hence, where the real work lies *inter alia,* is in the enforcement of the basic laws we

already have. Meaningful recommendations on the effective preservation and protection of the patient's privacy in the Nigerian health sector are outlined below.

8.1. Periodic Training of Health Personnel on Legal Intricacies in the Management of Patients' Medical Records. organized by the Nigeria Data Protection Commission in collaboration with the Health Records Officers Registration Board of Nigeria. This with boost proper ethical and legal handling of patients' medical data and records.

8.2. Comprehensive Legislative and Regulatory Reforms. Presently, Nigeria lacks a unique health data protection law. Like what is obtainable in other advanced jurisdictions, enacting a dedicated health data protection law would meaningfully transform the handling of patients' data disclosed during medical consultations. Such law should specifically address: collection, storage, use, and disclosure of patient health information; patient rights over their own health data; obligations of healthcare providers, HMOs, and digital health platforms; and penalties for unauthorized disclosure of patient information.

Additionally, existing laws can be amended to specifically provide for the handling of patients' data due to its sensitive nature. Such laws include the Nigeria Data Protection Act 2023. For instance, incorporating into it health-specific regulations; designating patient health information as a special category of sensitive data requiring heightened protection; and such like. Also, the Medical and Dental Practitioners Act can be reviewed to explicitly codify doctor-patient confidentiality as a statutory obligation; define clear exceptions to confidentiality **(**e.g., public health emergencies, court orders) and lucidly establishing civil and criminal liability for breach of patient confidentiality by medical professionals.

8.3. Establishing specifically a Health Data Privacy Regulatory Authority. It would be practically helpful to create a dedicated health data privacy body or designate a specialized unit within the Nigeria Data Protection Commission (NDPC) and arming such bodies with functions that can include: monitoring compliance with health data protection laws; investigating complaints from patients; imposing sanctions for violations; issuing guidance and best practice standards.

8.4. Develop National Electronic Health Records (EHR) Standards. In developed jurisdictions like USA there is in place a centralized structure for maintaining digital health records of patients. Replicating or establishing same in Nigeria would be very helpful with the following in place: establish mandatory EHR security standards for all healthcare facilities; require role-based access controls to limit who can view patient records; mandate audit trails for all access to electronic patient records

8.5. Require regular cybersecurity assessments of health information systems. This can be achieved through the adoption of a National Healthcare Cybersecurity Framework aligned with international standards. This will go a long way in handling the digital security of patients' vital data. Additionally, hospitals and clinics to implement the following: firewall and intrusion detection systems; data encryption at rest and in transit; regular penetration testing; and incident response plans for data breaches.