NIGERIA

ACRONYMS

4IR	Fourth Industrial Revolution
AI	Artificial intelligence
BCR	Binding corporate rules
ECOWAS	Economic Community of West African States
GRID	Geo-Referenced Infrastructure and Demographic Data for Development
HAGF	Honourable Attorney General of the Federation
ICT	Information and communication technology
IMEI	International mobile equipment identity
IMSI	International mobile subscriber identity
IoT	Internet of Things
IP	Internet protocol
MAC	Media access control
ML	Machine learning
MTA	Material transfer agreement
NASRDA	National Space Research and Development Agency
NDPA	Nigeria Data Protection Act
NDPR	Nigerian Data Protection Regulations, 2019
NITDA	National Information Technology Development Agency
PI	Principal investigator
PII	Personal identifiable information
SHR	Shared health record

MODES OF INFORMED CONSENT

This section provides legal clarity on the modes of informed consent. When data such as genomic data and personal health data are used in health research, clarity is needed on the modes of informed consent (e.g., broad, tiered or open consent) that are legally required from research participants in relation to data collection, analysis, storage, combination, sharing within a jurisdiction, and cross-border sharing.

There is no general data protection legislation. The National Information Technology Development Agency's (NITDA) Nigeria Data Protection Regulations, which is subsidiary legislation, fulfils this role. Health data is classified as sensitive personal data.

National Information Technology Development Agency (NITDA) Nigeria Data Protection Regulations

Types of consent

NITDA's Implementation Framework prohibits implied and bundled consent. Explicit consent, where the data subject ticks a box, signs a form or sends an email is required for the processing of sensitive data.

There is no research exemption provision.

When consent is required

Consent is required during collection and processing for a specific, legitimate and lawful purpose. However, consent may not be required for further processing for scientific research purposes. Consent is one of the conditions for lawful processing of personal data for one or more purposes.

When procuring consent or processing data

While procuring consent, data must not be obtained from a data subject unless the specific purpose of collection is made known to him or her. The data controller must also ensure that the consent of a data subject is obtained without fraud or coercion. Where processing is based on consent, the data controller must demonstrate that the data subject has consented and that he or she had the legal capacity to give consent.

When consent includes other matters

If consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner that is clearly distinguishable from the other matters in an intelligible and easily accessible form, and using clear and plain language.

Withdrawal of consent

The data subject must be made aware of the right to withdraw consent in advance, but such withdrawal will not affect the lawfulness of any processing that occurred before withdrawal.

Using consent to facilitate data transfers

Consent is another way to transfer data to a foreign country in the absence of a decision by The Agency or the Honourable Attorney General of the Federation (HAGF).

INDIVIDUAL AND COMMUNITY RIGHTS IN GENOMIC DATA

This section provides legal clarity on the nature and content of individual and community rights. Legal clarity is needed on the respective rights of individual research participants and their communities (where appropriate) in genomic data, in particular. These rights potentially include benefit sharing, ownership, and co-ownership in intellectual property rights in discoveries.

Many rights relevant to human genomics research are protected, including the right to human dignity and sanctity of the person and the right to privacy. The law mandates the state to protect peoples' cultures in order to enhance human dignity and encourage development of technological and scientific studies. These rights are pronounced in the Constitution but are also implemented in legislation, regulations and policy guidelines.

Regulatory and Supporting Institutions

Several institutions are involved in regulating and supporting compliance with human genomic research. These include the:

- Federal Ministry of Health
- Federal Ministry of Information and Culture
- Federal Ministry of Science and Technology
- National Agency for Food and Drug Administration and Control
- National Biotechnology Development Agency
- Nigeria Institute of Medical Research
- Nigeria Institute of Social and Economic Research
- Policy Innovation Centre.

Individual and Community Benefit Sharing

The approach to benefit sharing is as follows. With respect to research on human participants, the research participant must be informed of the expected and potential benefits of the research during and after the research, if there are any incentives given to participation, and the availability of beneficial products or interventions after the research is completed. There must be reasonable efforts to ensure that the benefits of research are made available to the community where the research was conducted. This is because the law requires that groups, communities, participants and researchers which bear the burden of research should share in the benefits.

Research must show value to the research participants and the community where the research was conducted. The research must be integrated with comprehensive capacity building, technology transfer and healthcare delivery strategies that address the significant local health problems of the community where it is undertaken. In addition, intellectual property, indigenous knowledge and contributions of all parties must be considered, adequately protected and compensated, especially where research leads to benefits. Therefore, before initiating a study/research, the mechanism of benefit sharing must be outlined in the form of benefit sharing agreements, MTAs, patent rights, and intellectual property and royalties' distribution agreements.

Benefits

(1) Tissue donation, removal and associated payment

For any tissue, organ, blood or gametes to be removed from any person, that person must give written consent. However, tissue, organ, blood and blood products or gametes may not be removed for merchandise, sale or commercial purposes. A donor can receive compensation for costs incurred in the process of making the donation. The amount paid as compensation must not exceed an amount which is reasonably required to cover the costs involved in the importation, export, acquisition or supply of the tissue, gamete, blood or blood product in question.

Purpose is limited to:

- Advancement of health sciences

- Health research
- Production of a therapeutic, diagnostic or prophylactic substance
- Therapeutic purposes, including the use of tissue in any living person
- Training of students in the health sciences.

(2) Patenting

While patenting is allowed, several inventions are not available for patenting. These include inventions considered to be contrary to public order or morality or which are prohibited by law, and also discoveries that are scientific in nature. The law does not mention patents relating to human genetic material.

GEOSPATIAL DATA FOR PUBLIC HEALTH SURVEILLANCE

This section provides legal clarity on the use of persons' geospatial data for public health surveillance. Web Geographic Information Systems are increasingly being used in public health surveillance involving infectious diseases. Privacy risks associated with the use of novel geospatial technologies (and the data generated by such technologies) are analysed and legal clarity is provided on how to comply with the law.

Pertinent legislation, regulations, guidelines and policies are discussed below.

General Framework

Legislation

For several years, data protection in Nigeria was partly regulated under the Nigerian Data Protection Regulations, 2019 (NDPR). However, the Data Protection Act (2023) now replaces the NDPR and the NDPR Implementation Framework 2019 issued under the National Information Technology Development Agency (NITDA) Act.

Despite the potential of digital contact tracing, it always conflicts with patient data privacy regulations. Nigeria's response complies with the NDPR, and it is possible to leverage call detail records to complement current strategies in the NDPR. The position under the NDPA (see below) would be similar.

Nigeria Data Protection Act

The Nigeria Data Protection Act (NDPA) establishes a Data Protection Commission headed by a National Commissioner to enforce compliance with the NDPA. Although the NDPA does not define personal data, its predecessor, the Data Protection Regulations, *define personal data as*:

> any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location

> data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; it can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifiers such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others; and

Personal identifiable information (PII) is defined as:

> information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in a context.

Geospatial data, such as location data and a person's address, are therefore personal data that can identify an individual, and therefore are subject to protection under the Regulations:

> It is the Data Protection Act that imported a definition for sensitive personal data which is defined as 'data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trade union membership, criminal records, or any other sensitive personal information'.

Accordingly, it seems that geospatial data can be considered as special personal information only if a person's address or location data (personal data) can also identify such a person's 'race' or 'ethnicity'.

Unlike the NDPR, *the NDPA further sets out several criteria for processing sensitive personal data*. It stipulates that a data controller or data processor must not on its behalf process, or permit a data processor to process, sensitive personal data, unless the:

> (a) data subject has given and not withdrawn consent to the processing for the specific purpose or purposes for which it will be processed;

(b) processing is necessary for the purposes of performing the obligations of the data controller or exercising the rights of the data subject under employment or social security laws or any other similar laws.

The NDPA also states that the newly established Data Protection Commission may issue directives prescribing further categories of personal data that may be classified as sensitive personal data. In this context, it is therefore possible for the definition of special personal data to be extended to also include geospatial data.

These provisions and the additional protections applicable to sensitive data merit careful consideration by health researchers combining geospatial data with health data in such a way that individuals may be identifiable.

The NDPA permits processing of personal data with the consent of data subjects, but as with the 2019 Regulations, it contains the provision that:

(3) Silence or inactivity of the data subject shall not constitute consent. (6) A request for consent shall be in clear and simple language and accessible format.

(7) Consent –

(a) shall be in the affirmative, and not based on a pre-selected confirmation; and

(b) may be provided in writing, orally, or by electronic means.

The clause "silence or inactivity of the data subject shall not constitute consent" has serious consequences when it comes to the covert surveillance of people or the collection of their geospatial or location data via remote sensors without them knowing and actively consenting to its collection. In these circumstances, consent cannot be relied upon, and another legitimate basis for processing the data must be established. In addition to these provisions, sensitive data is subject to additional protections.

Geospatial data in certain circumstances, such as where it is linked to health data of identifiable individuals, can be considered sensitive data and therefore must be regulated in terms of these

provisions. Processing is permitted with consent, but the NDPA does not contain an exemption for processing on public interest grounds, including scientific research. What is important is that in the case of research, the NDPA stipulates that the processing must take place in terms of a law which must be proportionate to the aim pursued and provides for suitable and specific measures to safeguard the fundamental rights, freedoms and interests of the data subject.

There is a broader exemption for processing to take place without consent where it is necessary for reasons of public health. The processing does not require an authorising law, but must implement privacy safeguards. This would include tracking, tracing, treatment and management of health emergencies or pandemics as lawful uses of health data without specific consent.

National Space Research and Development Agency Act (NASRDA)

NASRDA formally established the National Space Research and Development Agency, empowering the National Space Council as the regulating and supervisory entity for space activities in Nigeria.

Some of the functions of the Agency, as provided for in the Act, include:

- Develop satellite technology for various applications and operationalise the indigenous space system for providing space services and with the responsibility for building and launching satellites.
- Be the repository of all satellite data over Nigeria's territory and, accordingly, all collaborations and consultations in space data-related matters in Nigeria must be undertaken by or with the Agency.
- Promote the coordination of space application programmes in order to optimise resources and develop space technologies of direct relevance to national objectives.
- Encourage capacity-building in space science technology development and management, thereby strengthening the human resources development required for the implementation of the space programmes.

Draft Legislation, Guidelines and Policies

National Health ICT Strategic Framework

Digital health policy in Nigeria is articulated in the National Health ICT Strategic Framework. Although the framework does not mention the use of geospatial data, it does indicate significant work in digitising medical facility registry information which will implicitly rely on geospatial data as part of supply chain planning and verifying the location of patients' clinical interactions.

Geo-Referenced Infrastructure and Demographic Data for Development (GRID) programme

Nigeria's GRID programme is part of a bigger global initiative which aims to improve access to data for decision-making in all participating countries.

Conclusion and Recommendations

Nigeria has a Data Protection Act but has not developed laws to regulate the use of geospatial data. Although space research and e-Health policies greenlight the use of geospatial data, work remains to be done to overcome barriers in fully realising the potential benefits for universal healthcare delivery in Nigeria, while also respecting data privacy.

CROSS-BORDER SHARING OF DATA

This section reviews the rules as required by data protection law in the cross-border sharing of personal data. The rules on the cross-border sharing of personal data under data protection law do not exist in a vacuum, and therefore other important information that must be followed when sharing personal data is discussed. This information, however, is comprehensive as it relates to the cross-border sharing of personal data.

The relevant national health research regulations as they relate to the cross-border sharing of personal data are reviewed. These national health research regulations set out the required legal and ethical conditions that must be met when processing personal data for research. Applicable national legal and ethical documents are listed, but the discussion only specifies the requirements as they relate to the cross-border sharing of personal data for research. The guide does not treat the legal and ethical requirements generally required for research, and therefore users of this guide must consult with these documents to ascertain these requirements and to ensure that they are met.

An overview of the data protection law is provided. This includes what data the law applies to, the categories of data, the key individuals in the NDPA, the key principles required to be met in the processing of personal data, and the rights of data subjects. This is an overview only to help users to understand *some* of the requirements of the NDPA and to begin to assist users in navigating the NDPA. It is not comprehensive, and users of the NDPA must consult it to understand all relevant and applicable requirements to be met, and to understand any exceptions that may be in place for research. This is necessary as all these requirements must be met in the processing of personal data for research, in addition to the requirements on cross-border sharing of data.

The section provides users with a comprehensive description of the requirements to be met in the cross-border sharing of personal data for research. It sets out all the necessary conditions that must be met to legally share data across borders for research.

In countries where no data protection law is in force, the necessary national legal and ethical requirements, as they relate to the cross-border sharing of data, are presented.

The cross-border sharing of data is governed by several legal and ethical regulations, all of which must be met prior to the sharing of data for research. The Nigeria Data Protection Act (NDPA) is in force. It is a general data protection law that applies to the processing (i.e., use) of personal data in all sectors. Therefore, it is not a regulation that was introduced to regulate research. As

research processes vast quantities of personal data, the NDPA applies but it is only one of several laws that must be complied with when transferring data for research.

Health Research Regulations and Cross-Border Data Sharing

In addition to the national laws listed below, several international treaties and conventions have been signed. Of importance in this domain is the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) and the Supplementary Act A/SA. 1/01/10 on Personal Data Protection within ECOWAS (the ECOWAS Data Protection Act 2010). Nigeria has not ratified the Malabo Convention.

The relevant national legislation and guidelines are the:

- Constitution of the Federal Republic of Nigeria
- National Health Act
- National Code of Health Research Ethics 2007.

These laws set out the legal and ethical requirements that must be met for the conduct of research in Nigeria. There are no extra requirements for the cross-border sharing of data in this legislation.

Nigeria Data Protection Act

In addition to these legal and ethical requirements, the NDPA applies to the processing of all personal data, but in acknowledging the importance of research, special provisions are in place that deal with the processing of data purely for research purposes. The Nigeria Data Protection Regulation (NDPR) (and other legal instruments made by the National Information Technology Development Agency or the Nigeria Data Protection Bureau) was not repealed by the NDPA. The NDPR is still in force unless the relevant section conflicts with the NDPA. Therefore, it is arguable that the NDPR can be used to supplement the NDPA where there is the need for further clarity on the criteria set out in the NDPA.

The conditions set out in the NDPA must all be met for research. In addition, extra conditions must be met prior to the transfer of personal data across borders.

Some of the techno-legal terms used in the NDPA are discussed below. This is not a thorough assessment of the NDPA as it applies to research, but rather an overview of some of the key terms and conditions that must be met in the processing of personal data for research.

The Main Actors Defined in the Nigeria Data Protection Act

	Legal definition	**Layman explanation**
Data subject	An individual to whom personal data relates.	This is the person to whom the data relates.
Data controller	An individual, private entity, public commission, agency or any other body which, alone or jointly with others, determines the purposes and means of processing of personal data.	This is the person who decides what the data will be used for in research. Legal responsibility falls on the PI *and* on the research institution (as employer).
Data controller or data processor of major importance	A data controller or a data processor who is domiciled, resident in or operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria, as the Commission may prescribe, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Nigeria, as the Commission may designate.	
Data processor	An individual, private entity, public authority or any other body that processes personal data on behalf of or at the direction of a data controller.	This is someone who is not directly employed by the data controller but who processes personal data under the direction of the data controller (e.g., a consultant).
Data Protection Officer	Not defined in the NDPA.	An individual who ensures that an institution complies with the NDPA.

Commission	The Nigeria Data Protection Commission established under the NDPA.	This is the independent body that is established to monitor and enforce compliance with the law.

Categories of Data Listed in the Nigeria Data Protection Act

	Legal definition	**Layman explanation**
Personal data	Any information relating to an individual, who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual	This is data/information about a particular person, which can identify him or her.
Sensitive personal data	Personal data relating to an individual's (a) genetic and biometric data, for the purpose of uniquely identifying a natural person; (b) race or ethnic origin; (c) religious or similar beliefs, such as those reflecting conscience or philosophy; (d) health status; (e) sex life; (f) political opinions or affiliations; (g) trade union memberships; or h) other information prescribed by the Commission as sensitive personal data under the NDPA.	This is personal data relating to or information about a particular person which is considered sensitive, such as health data and genetic data, and which receives additional legal protection.
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological, or behavioural characteristics of an individual, which allow or confirm the unique identification of that individual, including without limitation by physical	

	measurements, facial images, blood typing, fingerprinting, retinal scanning, voice recognition and DNA analysis.	
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.	This is a kind of processing where the direct identifiers of personal data are removed (e.g., a name) so that it is impossible to identify the person without adding other information. This is often called coded data. Data protection law still applies to pseudonymised data.

The NDPA applies to the processing of personal data

Generally, data protection law applies only to personal data. This is data that refers to an identified or identifiable person. For data that does not fall under the definition of personal data, the data protection law does not apply. The NDPA applies specifically to the processing of personal data.

De-identification and pseudonymisation of personal data

The NDPA refers to de-identification and pseudonymisation. Pseudonymisation is when information is removed from the data so that it is impossible to identify an individual and that information is kept separately by using technical and organisational measures. Data that has been pseudonymised does fall under the NDPA.

Although de-identification is mentioned in the NDPA, it is not defined. De-identification is one of the technical and organisational measures which a data controller may employ to ensure the security, integrity and confidentiality of the personal data in his/her control, in order to guard against inter alia misuse, unauthorised disclosure, or access. In the absence of specific guidance and clarity in the alternative on this point, it seems that de-identified data falls within the NDPA.

If a data controller uses pseudonymisation and de-identification techniques, the data controller is required to regularly test that the measures employed are effective, updated when necessary and

that any new measures are instituted to address any shortcomings in current methods or to address new risks.

Categories of personal data

Data that is not personal data does not fall under the NDPA. While the exact parameters of what is non-personal is unclear from the NDPA, several types of data are clearly considered personal:

- personal data;
- sensitive personal data (including biometric data);
- pseudonymised data; and
- de-identified data.

The first three types of data (personal, sensitive personal (including biometric) data and pseudonymised data) are defined and an assessment would need to be made to consider whether the data falls under these definitions. Unfortunately, given the lack of a definition of de-identified data, it is unclear what qualifies as de-identified data. Furthermore, whether pseudonymisation is merely a safety measure, or whether it amounts to non-personal data in the hands of the data recipient, who does not have access to the identifying data set, is unclear.

In the absence of a test or clear guidance from the Authority, the following can be clearly ascertained from the NDPA and by drawing on tests in other jurisdictions:

Recommended test: Ask yourself:

1. Is the data able to, directly or indirectly, individually identify a data subject, in reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual?
2. Is the data able to be linked with other data kept separately, in order to identify a data subject, either directly or indirectly?
3. Is the method used to de-identify the data subject reversible?

4. Is there any reasonably foreseeable method that could be used by someone to identify the data subject directly or indirectly by employing methods such as linking it to other data, or manipulating the data, or any other novel methods?

If the answer is "Yes" to *any* of these questions, the data is *personal data* and will fall within the ambit of the NDPA. If the answer is "No" to *all* of these questions, then this data will most likely be non-personal data and will fall outside the scope of the NDPA.

Special Note on Genetic and Genomic Data

Genetic data is considered to be sensitive data. It has a higher level of protection under data protection law. There is ongoing debate about whether genomic datasets can ever truly be considered not to be personal data, in particular as genetic data is an identifier.

In its definition of genetic and biometric data, the NDPA provides that genetic data is sensitive data where it is "for the purpose of uniquely identifying a natural person" and where it allows or confirms "the unique identification of that individual". Therefore, in deciding whether a genomic dataset can be considered to fall outside of the definition of personal data, context matters. Therefore, consider whether the data allows for anyone to identify the data subject.

Key Principles That Must be Met in Terms of the Nigeria Data Protection Act

1. *Lawfulness, fairness, and transparency:* A data controller or data processor must ensure that personal data is processed in a fair, lawful and transparent manner. Lawful means that there must be a legal basis for the processing of the personal data as set out in the NDPA. Genetic (and biometric) data is considered to be *sensitive personal data*. Generally, the processing of sensitive personal data including genetic data is prohibited unless the processing is for certain purposes including medical care or community welfare (to be carried out by a healthcare or similar service provider bound by a duty of confidentiality), public health and scientific research.

2. *Purpose limitation:* Personal data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Special provisions deal with purpose limitation, for example, "further processing for archiving purposes in the public interest, scientific, historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes".
3. *Adequacy:* Personal data must be adequate, relevant, and limited to the minimum necessary for the purposes for which the personal data was collected or further processed.
4. *Storage limitation:* Personal data should be retained for not longer than is necessary to achieve the lawful bases for which the personal data was collected or further processed.
5. *Accuracy:* Personal data must be accurate and, where necessary, kept up to date. Processes should be in place to ensure that all personal data collected is accurate.
6. *Security safeguard:* Personal data should be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach.
7. *Security, integrity and confidentiality:* A data controller and data processor must implement appropriate technical and organisational measures to ensure confidentiality, integrity and availability of personal data.
8. *Accountability and duty of care:* A data controller or data processor owes a duty of care to the data subject in respect of data processing and must demonstrate accountability in respect of the principles contained in the NDPA.

Data Subject Rights in Terms of the Nigeria Data Protection Act

Data subjects have rights that the data controller must protect. These rights are:

(1) *Right to be informed:* The data subject has the right to confirm whether the data controller or processor is storing or processing his/her personal data. When a data controller is processing personal data, a data subject has the right to be informed of the purposes of the processing, the categories of personal data concerned, the recipients or categories of recipients who the personal data has been or will be disclosed to, *particularly* recipients in third countries or

international organisations and for how long the data will be stored. Furthermore, where personal data is not collected directly from the data subject, the data subject has the right to be informed about its source.

(2) *Right to rectification and erasure:* A data subject has the right to request from the data controller rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject, or to object to such processing.

(3) *Right to lodge a complaint:* A data subject has the right to lodge a complaint with the Commission.

(4) *Rights in relation to automated decision-making and profiling:* A data subject has the right to be informed about the existence of automated decision-making, including profiling, and its significance and envisaged consequences. Furthermore, the data subject has the right not to be subject to a decision based solely on automated processing of personal data, including profiling, and which produces legal or similar significant effects concerning the data subject.

(5) *Right of access:* The data subject has a right to obtain a copy of his/her personal data that the data controller has in his/her possession or who is processing such data in a commonly used electronic format. An exception is when providing such data would impose unreasonable costs on the data controller. In such a case, the data subject may be required by the data controller to bear some or all such costs.

(6) *Right of correction and erasure:* The data subject has the right of correction, or if correction is not feasible, deletion of his/her personal data that is inaccurate, out of date, incomplete or misleading. The data subject also has the right to erase personal data concerning him/her and to restrict data processing in certain circumstances.

(7) *Right to withdrawal of consent:* A data subject must have the right to withdraw consent to the processing of his/her personal data at any time. This will apply where consent is the lawful basis of processing.

(8) *Right to object:* A data subject must have the right to object to the processing of his or her personal data and the data controller must discontinue the processing unless the data controller can demonstrate a public interest (not defined) or other legitimate grounds which override the fundamental rights and freedoms and interests of the data subject. Likewise, a data subject has a right to object to the processing of his or her personal data for direct marketing purposes, including profiling.

(9) *Right to data portability:* A data subject has the right to data portability. Therefore, a data subject can receive personal data concerning him/her in a structured, commonly used, and machine-readable format from the data controller and the personal data can be transmitted without any hindrance directly from one data controller to another where technically possible.

Cross-Border Data Sharing

The NDPA also has additional provisions in place that must be met when personal data is to be transferred outside of the country. These additional provisions are in place to ensure that data subjects continue to be protected once the data leaves the country.

Cross-border transfers of personal data are not defined in the NDPA, but provisions on cross-border data sharing would apply when the data is being sent to a data controller in another country. It could also *arguably* include where a researcher outside of Nigeria is given access to the personal data stored in a database, biobank or cloud that is hosted in Nigeria.

Requirements for lawful transfer of data outside of Nigeria

To transfer personal data outside of Nigeria under the NDPA, there must be a lawful basis for this transfer. This can be one of the following:

1. The recipient of the personal data is subject to a law, binding corporate rules (BCR) or contractual clauses, code of conduct or certification mechanism that affords an adequate level of protection to personal data in accordance with the NDPA. The data controller or processor must:
    a. Establish the basis of the cross-border transfer of personal data in terms of the conditions stipulated; and
    b. Determine, through an assessment, whether the level of protection afforded by the recipient country is "adequate" for the purposes of the NDPA.

Considerations when considering adequacy

In considering adequacy, the data controller or processor can consider:

- the availability of the data subject's enforceable rights and ability to enforce such rights through administrative and judicial redress;
- the availability of any appropriate instrument in place between the Commission and a competent authority in the recipient jurisdiction that guarantees 'adequate' data protection;
- access of the public authority to personal data;
- the existence of an effective data protection law;
- the existence of an independent and competent data protection or similar supervisory authority;
- the relevant country being bound by international commitments or conventions and its membership of any multilateral or regional organisations.

Regarding determining adequacy of the law in the recipient country, the list developed by NITDA in the NDPR Implementation Framework is applicable.[1]

Other legal bases that can be relied upon in the absence of adequacy

1. The data subject consents to the transfer of personal data outside of Nigeria. The data subject must be informed about the possible risks of such transfer in the absence of adequate protections.
2. The transfer is necessary for the performance of a contract to which the data subject is a party or it is necessary to take steps at the request of a data subject before entering a contract.
3. The transfer is for the sole benefit of a data subject and it is impractical to get the consent of the data subject. Furthermore, if the data subject were able to give consent he/she would most likely have provided this consent.
4. The transfer is necessitated by important public interest reasons. The NDPA does not, however, define public interest.

[1] Annexture C 'Countries deemed as having adequate data protection laws' Nigeria Data Protection Regulation 2019: Implementation Framework https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf

5. The transfer is necessary for the establishment, exercise, or defence of legal claims.
6. The transfer is necessary to protect the vital interest of the data subject or of other persons where a data subject is physically or legally incapable of giving consent.

LEGAL REGULATION OF AI

This section develops/pioneers an approach to the legal regulation of artificial intelligence (AI) in health discovery and innovation. Data science in health research is increasingly used with AI applications that can transform health innovation. This requires robust governance, risk assessment strategies, and mechanisms to protect human rights

There is no specific AI legislation in Nigeria and no particular legislative provision that addresses AI-related issues, including predictive algorithms. Therefore, it is necessary to consider the legal landscape on AI development and use. Five thematic areas considered most relevant to AI regulation are explored: (1) AI policy documents; (2) Digital/E-Health and medical device regulation; (4) Consumer protection and ICT/E legislation (3) Data protection law; and (5) Intellectual property.

AI Strategy

Nigeria has not yet formulated an AI framework, policy or strategy. Its National Cloud Computing Policy (Cloud Policy) sets out to develop the manner in which information is processed in the electronic sphere in order to promote Nigeria's digital growth. This is because appropriate processing power and storage capacity is vital to enable 4IR technologies.

National Cloud Computing Policy

The Cloud Policy provides definitions for AI, machine learning and the Internet of Things. The provided definitions clearly delineate hardware and software components of 4IR technologies. AI is understood to suggest the creation of intelligent objects, while ML refers to the underlying algorithm and programming. Both definitions underscore the absence of human intervention. Instead, IoT emphasises the real-world application and interoperability of these technologies via digital platforms in a bid to help humans with automatic decision-making.

The Cloud Policy aims to increase adoption of – and investment in – cloud computing by organisations providing digital-enabled services to the government. It intends to do so by creating an enabling environment for investment in infrastructure, by providing clear direction and programmes and ensuring an enabling and competitive environment for national cloud service providers.

Digital Health/E-Health

Nigeria has a legal framework for dealing with health and research. This includes the:

- National Health Act (the Act).
- National Health ICT Strategic Framework 2015–2020 (the Framework) or the eHealth Strategy for Nigeria.
- National Health Policy (the Policy).

These cover the National Health Research and Information System. The National Health ICT Strategic Framework envisions a shared health record (SHR) that will ensure that health information from patients is stored and collected in a repository and thereafter that this data can be shared with other health institutions. The National Agency for Food and Drug Administration and Control also oversees the health sphere as it pertains to medical devices.

Nigeria has no specific legislation dealing with AI in healthcare.

Consumer Protection and ICT/E-Legislation

Consumer Protection	Federal Competition and Consumer Protection Act
ICT/E-Legislation	The Nigerian Communications Act and the proposed Cybercrimes (Prohibition, Prevention, etc.) Act appear to be the only ordinances that govern the electronic sphere

Data Protection Law

The data protection law is the Nigeria Data Protection Act (NDPA) (2023) and the Nigerian Data Protection Regulations (2019).

The NDPA applies to both automated and non-automated processing. The data controller should make the data subject aware of the existence of automated decision-making, including profiling, prior to the collection of personal data. In addition, the data controller should provide meaningful information about the logic involved, and the significance and envisaged consequences of such processing.

Processing of sensitive data can occur only if certain conditions are met.

Intellectual Property

The Copyright Act and Patents and Designs Act govern the protection of intellectual property and related matters in Nigeria.

Summary and Analysis

Particularly important is the Nigerian Cloud Computing Policy, which would constitute a vital component in a 4IR-enabling infrastructure base. While several policy documents guide digital heath implementation, no specific legislation provides for AI use in healthcare. The above policy documents are interoperable and do not supersede one another. However, relevant provisions in promulgated legislation will take precedence over other regulatory/policy documents.

The NDPA and the Nigerian Data Protection Regulations, 2019 provide for the automated and non-automated processing of data. Of note are the rights of the data subject – and the processing of sensitive data where certain conditions are met.

Those purchasing AI technologies are unlikely to find much protection under the Federal Competition and Consumer Protection Act. However, ICT/E-legislation and a consideration of intellectual property legislation, jurisprudence and soft law may be essential in ensuring that these technologies are utilised properly.