THE GAMBIA

ACRONYMS

4IR	Fourth Industrial Revolution
AI	Artificial intelligence
DPA	Data Protection Act
ECOWAS	Economic Community of West Africa States
GDPR	General Data Protection Regulation (Europe)
GIS	Geographical information system
ICA	Information and Communications Act
ICSP	Information and communications service provider
ICT	Information and communication technology
ICT4D	ICT for Development
IPR	Intellectual property rights
IT	Information technology
MDEG	Methyl-Donors and EpiGenetics in The Gambia
MOICI	Ministry of Information and Communication Infrastructure
NDP	National Development Plan
NSTIP	National Science, Technology and Innovation Policy
PI	Principal investigator
PURA	(The Gambia) Public Utilities Regulatory Authority

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 to guide scientists conducting health research. An Information and Communications Act provides for the processing of personal data and protection of privacy, but applies only to processing by information and communications service providers.

Draft Data Protection and Privacy Policy Strategy

The relevant instrument that health research scientists should heed is the Draft Data Protection and Privacy Policy Strategy. The Policy is not binding but is important because it will be used to, among other things, inform the development of data protection and privacy law to safeguard personal data and the rights to data protection and the privacy of individuals.

The Policy provides, among other things, that personal data must be lawfully processed and have a legitimate basis. This requires, among other things, that processing of personal data be based on the data subject's consent. Such consent must be freely given, specific, informed and unambiguous.

The Policy also allows for the transfer of personal data outside of the country to take place if the data subject has given explicit, specific and free consent, after being informed of risks in the absence of appropriate safeguards.

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.

There is no meaningful legal and legislative framework regulating human genomic research. The Constitution Promulgation Bill was rejected by the National Assembly in 2020.

Regulatory and Supporting Institutions

A number of institutions are, however, involved in regulating and supporting compliance with human genomic research. These include the:

- Joint United Kingdom (UK) Blood Transfusion and Tissue Transplantation Services Professional Advisory Committee
- Medical Research Council Unit The Gambia at London School of Hygiene and Tropical Medicine
- Methyl-Donors and EpiGenetics in The Gambia (MDEG)
- Ministry of Health and Social Welfare
- The Gambia Public Utilities Regulatory Authority

Individual and Community Benefit Sharing

The approach to benefit sharing is as follows. Research participants must be adequately informed of the kinds of benefits and compensation that come with participating in the research activity, although there is no clear definition of what those benefits are. According to the Medical Research Unit, a research study may be of no direct benefit to the research participant. However, research is meant to help health professionals learn more about a disease or condition being investigated and how to control it in order to help people suffering from that disease or condition to have better treatment in the future.

Benefits

(1) Tissue donation, removal and associated payment

No definite laws and guidelines regulate biomedical research. Legislation is limited and inaccessible.

(2) Patenting

Patenting is allowed and encouraged, but a number of inventions are not available for patenting. These include discoveries, scientific theories and mathematical methods; methods for the treatment of the human or animal body by surgery or therapy, as well as diagnostic methods practised on the human or animal body – and this provision does not apply to products for use in any of those methods. 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.

The legal framework for regulating the lawful use of geospatial data is largely absent, and there is no information publicly available on how the government of The Gambia intends to develop legislation, policies or guidelines on the use of GIS data either generally or specifically in relation to healthcare services and health research.

General Framework

Legislation and Associated Structures

The Gambia does not have any promulgated data protection laws nor any laws dealing with geospatial data. The closest legislation that deals with similar issues is the Information and Communications Act.

Provisions of the Information and Communications Act (ICA)

- The ICA aims to provide for the restructuring, development and regulation of the information and communications sector in The Gambia and for related matters. Data protection/privacy rules stipulated in the ICA relate primarily to information and communications service providers (ICSPs). The ICA applies to all information and communications services and systems as defined in the ICA, other than those exempted under it.

- It provides that the government must guarantee the independence of the competent authorities with respect to all organisations providing networks, equipment or services in the information and communications sector and also ensure complete and effective separation of the regulatory function from the activities associated with ownership or control. The

Gambia Public Utilities Regulatory Authority (PURA), working with the government, must regulate the information and communications sector based on the principles of the ICA.

- ICSPs must be authorised to process personal data in connection with billing charges for information and communications services, to the extent required and necessary for calculating and billing charges, in particular the data relating to the date, duration and place of the service to which it pertains. ICSPs may also process the type of personal data which is technically essential for the provision of services.

- ICSPs must use in their operations for providing information and communications services only the type of information and communications apparatuses which has sufficient facilities to ensure that personal data is processed only where it is absolutely necessary in terms of the provision of services and for the implementation of other objectives specified in the ICA.

- ICSPs must delete any personal data from their records that is used for purposes other than those defined in the ICA. The provision of information and communications services must not depend on the user providing consent for processing his or her personal data for purposes other than those defined in the Act.

- ICSPs must enable the end-users to have access to information concerning the type of personal data the service provider is processing and the objectives – at any time before and during the use of the information and communications services.

- The ICA provides that the national security agencies and investigating authorities may monitor, intercept and store communications, and the Authority, when exercising its powers conferred relating to frequency monitoring, may otherwise intrude on communication for surveillance purposes. From a geospatial data privacy perspective, this may be problematic because people could be identified and targeted for purposes known only by the surveyors.

- If an alleged threat of murder or physical violence or blackmail occurs, the user or subscriber threatened may authorise the investigating authority to intercept telephone conversations,

other information and communications, email messages and any other form of communications on his or her end terminal to investigate and to identify the persons involved in communications within the period of time set in the user's authorisation. The Minister may determine that information and communications operators and service providers must implement the capability to allow the authorised interception of communications. The intrusion into another person's privacy may be authorised by law.

- ICSPs must take appropriate technical and organisational measures to block any unauthorised attempt to intercept, store or monitor communications transmitted and any related traffic data and to prevent any unauthorised or accidental access to communications transmitted and any related traffic data. These can be construed as a measure taken to protect the privacy of people.

- ICSPs must use in their operations for providing information and communications services only the type of information and communications apparatuses that have sufficient facilities to ensure the privacy of communications. ICSPs must be authorised to obtain and store communications transmitted on their network only to the extent absolutely necessary for the provisions of services for technical reasons.

- Information obtained via information and communications networks may be stored on electronic communication terminal equipment, or accessed only on the end-users' and subscribers' prior consent granted after being in possession of clear and comprehensive information about the implications.

- ICSPs must take appropriate technical and organisational measures to safeguard the security of their services. The technical and organisational measures must be sufficient with regard to best practices and the costs of the proposed measures, to offer a level of security that is appropriate to the risk presented in connection with the services provided.

- In the case of a particular risk of a breach of the security of the services in spite of the technical and organisational measures taken, the service provider must inform the

subscribers of the risk and of the measures the subscribers may take to enhance the level of protection. In the case of an event affecting or jeopardising the security of the services, where a previously unknown risk of a breach of the security occurs as a result, the ICSP must inform the subscriber of the risk and of the measures the subscriber may take to enhance the level of protection, and also the estimated costs involved. However, the service provider must still take appropriate and immediate measures to restore the normal security level of the service.

- Where the provision of a value-added service requires that traffic or location data is forwarded, this refers directly to geospatial data. This pertains only to subscribers of the telecommunications service provider's services, and therefore not all or any person's geospatial data. The legal basis for this should thus be one of a contract. The service provider must inform the subscribers or users about the type of data required, the purpose and duration of data processing, and whether the data is to be forwarded to third persons.

- ICSPs must be authorised to process traffic or location data only on the prior consent of the subscribers or users to whom the data is related, and only to the extent and for the duration necessary for the provision of value-added services. Users and subscribers have the right to withdraw their consent at any time.

The Gambia Public Utilities Regulatory Authority

This Authority established under The Gambia Public Utilities Regulatory Authority Act must regulate information and communications services, information and communications networks, associated facilities, and associated services. However, the Information and Communications Act primarily deals with regulating ICT service providers. Therefore, the privacy rights under this Act are limited to application in the context of data collected by ICT service providers, or data gathered through interception of communication services. This Act does not apply to GIS data.

Cybercrime Bill

The Ministry of Information and Communication Infrastructure (MOICI) has launched a public consultation on a draft Cybercrime Bill. It expands the range of statutory offences from the limited criminal penalties in the Information and Communications Act. Once passed, this would apply

only to criminal activities and not to a bona fide health research projects that obtained the GIS data with appropriate permissions from the data holder.

The objectives of the Cybercrime Bill are to:

- protect the confidentiality, integrity and availability of computer systems, programs and data;
- prevent the unlawful use of computer systems;
- facilitate the prevention, detention, investigation, prosecution and punishment of *cybercrime*;
- facilitate international cooperation on matters covered under the Bill.

Unauthorised interception of computer data

A person who intentionally and without authorisation intercepts or causes to be intercepted any computer data to, from or within a computer system, commits an offence. A person convicted for this offence is liable on conviction, in the case of:

> (a) an individual, to a fine not exceeding two hundred thousand dalasis or imprisonment for a term not exceeding five years, or to both the fine and imprisonment;
> (b) a body corporate, to a fine of not less than five hundred thousand dalasis.

An act of interception of any computer data to, from or within a computer system, includes listening to, or recording, or acquiring the substance, its meaning or purport of that computer data.

Draft Policy

Draft Data Protection and Privacy Policy Strategy, 2019

The Public Utilities Regulation Authority (PURA) is a regulatory body that is to be created by the Draft Data Protection and Privacy Policy Strategy (the Draft Policy Strategy). However, this Policy does not have the status of law. Its purpose is to lay the foundations of an institutional and legal framework for data protection and privacy that will give effect to the Constitution and express the

commitment of the Government of The Gambia to ensure the protection of personal data and associated rights of individuals, and in particular the right to privacy. The Draft Policy Strategy will:

- apply to the processing of personal data in the private and public sectors, whether by automated or non-automated means and irrespective of the nationality or place of residence of the data subject;
- not apply to the processing of personal data made for personal or household purposes;
- apply to personal data or special categories of data about living individuals;
- apply to data processing undertaken in The Gambia.

The Draft Policy Strategy also seeks to establish a Gambian Data Protection Authority.

A key objective of the Policy is to identify an independent and impartial National Supervisory Authority (Supervisory Authority) appropriately empowered to oversee, monitor, and enforce compliance and safeguarding of the data protection and privacy rights of individuals. Under this Policy, the Supervisory Authority will be empowered by a Data Protection Act (DPA) as an independent administrative body. The DPA will ensure that the Authority is empowered as a statutory independent and impartial Authority, and cover the scope of its mandate, its powers, and ability to acquire property, sue and be sued.

Consistent with the Government of The Gambia's recognition of the right to privacy as a fundamental human right (as contemplated in the Constitution and the draft Data Protection and Privacy Policy, and by virtue of The Gambia being party to international human rights conventions), the DPA should expressly confirm that the Authority will treat the privacy of an individual as a fundamental human right.

The Authority is usually the institution mandated by the DPA to protect the rights of individuals and to protect their personal data, to determine the process by which it is processed and to ensure compliance with the provisions of the African Union Malabo Convention and Council of Europe Convention 108+. It will:

- have powers of investigation and intervention;
- perform the function of authorising and approving standardised safeguards relating to cross-border data flows;
- make determinations relating to violations of the DPA and impose the necessary administrative sanctions;
- instigate legal proceedings;
- issue opinions and approve statutory Codes of Conduct or Guidelines relating to the processing of personal data;
- publish reports of its activities.

The Authority's mandate should include the responsibility to take part in international cooperation to promote public awareness of its functions, powers and activities; the rights of data subjects and exercise of such rights; and awareness of controllers and processors about their legal obligations under the DPA, especially in processing special category data such as that of children and other vulnerable individuals. The Authority must be consulted on proposals for any legislative or administrative measures involving the processing of personal data, and requests and complaints from data subjects.

The principles outlined in the Policy are based on international best practice taking into consideration the Malabo Convention and the modernised (and most widely adopted globally) Convention 108+.

Personal data is not defined in the Policy, but once a data protection statute is adopted it can be assumed that geospatial data will be regarded as personal data where it makes it possible to identify and individual through, for example, location data.

Sensitive data is dealt with under Special Categories of Data. The processing of the following categories of data will be allowed only where appropriate safeguards are in place that complement those enshrined in the data protection and privacy law:

- genetic data;
- personal data relating to offences, criminal proceedings and convictions, and related security measures;
- biometric data uniquely identifying a person;
- personal data for the information it reveals about racial or ethnic origin, political opinions, trade union membership, religious or other beliefs, health or sexual life.

Safeguards will guard against risks that the processing of such data may present for the interests, rights and freedoms of the data subject, notably the risk of discrimination. Appropriate safeguards include, where the processing is carried out:

- with the data subject's explicit consent;
- under a professional secrecy obligation;
- because of a law covering the intended purpose and means of the processing or indicating the exceptional cases where processing such data would be permitted;
- by a particular and qualified organisation;
- when it is necessary to protect the vital interests of the data subject or of another natural person.

In the Policy, there is provision for data protection by design. The Policy provides:

Data protection and privacy by design and default

- Before carrying out processing, controllers (and, where applicable, processors), must examine its potential impact on the rights and fundamental freedoms of data subjects prior to the commencement of the processing, and must design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.
- Controllers (and, where applicable, processors), must implement technical and organisational measures which consider the implications of the right to the protection of personal data at all stages of data processing.

- This implementation of data protection requirements should be achieved not only as regards the technology used for processing the data, but also regarding the related work and management policies and processes.
- When setting up the technical requirements for default settings, data controllers and data processors should choose privacy-friendly standard configurations so that the usage of applications and software does not infringe the rights of the data subjects (data protection by default), and to avoid processing more data than necessary to achieve the legitimate purpose.

Data controllers should be aware of this provision and should not use geospatial data that identifies individuals for purposes other than what was initially stated or agreed upon without obtaining additional consent.

The rights to privacy and personal data are not absolute rights. They have to be balanced with other human rights (with the exception of the right to life and to human dignity) and may be subject to specific exceptions for the lawful processing of personal data undertaken for important public or private interests. The use of exceptions and restrictions must be subject to objective legal requirements to be considered lawful and to guard against their arbitrary application. According to objective criteria, all exceptions or restrictions have to be provided for by law, must pursue a legitimate purpose, respect the essence of fundamental rights and freedoms, and constitute a necessary and proportionate measure in a democratic society.

Rights of data subjects

Every individual must have a right:

- not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views considered;
- to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing;

- to obtain, on request, knowledge of the reasoning underlying the processing of personal data about them;
- to object, at any time, to the processing of personal data concerning him or her unless the data controller demonstrates legitimate grounds for the processing that override his or her interests or rights and fundamental freedoms;
- to obtain, on request, free of charge and without excessive delay, the rectification or erasure of such data processed contrary to the provisions of this policy and the proposed law;
- to obtain, on request, free of charge and without excessive delay, judicial and non-judicial remedy for violations of the law;
- to benefit, whatever his or her nationality or residence, from the assistance of the Supervisory Authority in exercising his or her rights.

The above will not apply if the decision is authorised by a law to which the data controller is subject, and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

The Draft Policy Strategy requires data controllers to notify at least the competent supervisory authority of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

Outlook for future data protection laws

Geospatial data is not referred to in the Draft Policy Strategy. However, as the Policy intends for data protection legislation to be modelled on the most recent global standards, guidance can be sought from countries that have a comparable framework, such as South Africa and the application of the Protection of Personal Information Act to geospatial data in South Africa. From this analysis, it can be predicted that when data protection laws are enacted in The Gambia:

1. The definition of personal data will refer to information relating to an individual who can be identified or can be deemed to be identifiable through factors specific to that individual's physical data. Such physical data can be construed to include an individual's location or geospatial data – the individual's physical address or presence at a certain place in time.

2. Sensitive personal data will be subject to heightened protection. Geospatial data may also qualify for protection as sensitive personal data where it reveals a natural person's property details or health data, such as state of physical or mental health of an individual, including the individual's future state of health, collected for purposes of providing health services, or data which associates the individual with the provision of specific health services. For example, during a national health emergency, the locations of individuals infected with an infectious disease may be collected for purposes of treating those persons and to track and trace the whereabouts or geolocations of the people with whom they had contact.
3. Geospatial data could be considered as a unique patient identification number where the location from which a patient came from or to where a patient may be returning is of vital importance for the management of an epidemic. In combination with the patient's ID, hospital or clinic number, this identification location may be different from any other identification number possessed by the data subject, which requires the data controller to take appropriate security safeguards. In such instances, a medical practitioner or healthcare provider could also breach the common law and/or statutory duty of confidentiality towards their patients by disclosing such information.
4. Consent by the data subject would be a ground for lawful processing of personal data, but other lawful grounds would be recognised. For example, if geospatial data is collected and used in a public health emergency, the individual's consent for its processing is not required, because such processing is carried out in the public interest.

   This is similar to the position in most countries that have adopted modern data protection legislation. Consent is but one of the legal grounds on which a data controller may process sensitive personal data, including geospatial data, of an individual. Other legal grounds for the lawful processing of sensitive personal information include if the individual has made the data public; if the processing is necessary for national security; if the processing is necessary for any reason of substantial interest to the public; or if the processing is necessary to protect the vital interest of a data subject or another person and where neither the individual nor anyone on his or her behalf can provide consent. Geospatial data can accordingly be lawfully processed when and where the health interest of the public is at stake. Health emergencies that qualify as epidemics or pandemics should constitute public

health interests of sufficient substance to allow for lawful processing of sensitive personal information.

Conclusion and Recommendations

The Gambia has no law that specifically deals with geospatial data. The protection of data privacy and confidentiality can be deduced from the broad interpretation of laws relating to electronic communication and the networks that make communication possible.

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.

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.

Generally, in most countries, 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. In The Gambia, there are limited regulations and/or guidelines in this domain. There is no data protection regulation in force.

Health Research Regulations and Cross-Border Data Sharing

The health sector regulatory landscape is policy heavy but light in law. Relevant policies and documents are:

1. The National Health Policy 2021–2030

2. The National Health Laboratory Services Strategic Plan 2021–2025
3. The Gambia ICT4D Policy framework
4. The National Science, Technology and Innovation Policy (NSTIP) (2013–2022)

Most of the policies recognise the importance of sharing data and international collaborations for the development of the health sector, without clearly stipulating any strategy for cross-border data sharing. The National Health Policy 2021–2030 seeks to promote health research in strategic areas but does not have a policy for cross-border flow of data for health research. The National Health Laboratory Services Strategic Plan 2021–2025 promotes data sharing among laboratories and agencies whose activities affect human health. It also encourages collaboration in implementing the One Health strategy. The One Health Model adopted by ECOWAS member states, including The Gambia, emphasises cross-border collaboration and information sharing among countries.

Data Protection and Privacy Policy and Strategy

Although The Gambia has no data protection law, the Data Protection and Privacy Policy and Strategy was adopted in 2019. A Data Protection Act is currently under development.

Miscellaneous Guidance

The African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) is in force. The Gambia has signed it, but has not yet to ratified it. However, it may guide researchers in adopting standards in data protection.

The Economic Community of West Africa States (ECOWAS) Supplementary Act on Personal Data may also be of guidance.

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 legislation on AI and no legislative provision addresses AI-related issues including predictive algorithms. Furthermore, there is no technological provision, industry- or sector-specific guidance in place. It is therefore necessary to consider the legal landscape for 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; (3) Consumer/ICT legislation; (4) Data protection law; and (5) Intellectual property.

AI Strategy

Several strategies concern digital transformation and innovation:

The Gambia National Development Plan (2018-2021)

The vision and overall goal of the NDP will be realised through eight strategic priorities, including: transforming the economy, developing infrastructure and making the private sector the engine of growth, transformation and job creation. These priorities are complemented by seven crosscutting critical enablers. There is a need to change The Gambia into a digital nation, by creating a modern information society and strengthening evidence-based policy, planning and decision-making.

The Gambia National Cyber Security Strategy and Action Plan 2020–2024

This strategy provides guidance on the development of a national cybersecurity ecosystem. This includes a legal, regulatory and institutional framework, building cybersecurity capacity and capabilities and the development of standards and guidelines to: (i) ensure that critical ICT systems

and infrastructure in public are protected and made resilient; and (ii) foster adoption of security standards and guidelines in the government and private sector.

The Strategy has the following five strategic goals:

- Establishing national risk assessment in order to protect critical national infrastructure. The Risk assessment will therefore consist of a national threat assessment, a vulnerability assessment, and an overall impact analysis.
- Building cybersecurity capabilities to enable risk control, mitigate vulnerabilities and determine the likelihood of threat occurrence and potential loss or damage.
- Develop institutional governance frameworks to ensure effective coordination of national cybersecurity initiatives.
- Promote national and international cooperation to enhance capacity-building, information-sharing, threat assessment, and joint management of cybersecurity programmes, incident reporting, and advocacy.
- Cybersecurity capacity-building and awareness with a focus on computer ethics, computer security, and incident reporting.

E-Government Strategy 2021–2024

The Strategy aims to create an integrated and secure online public service delivery framework. The principles of transparency, public service improvement, innovation and efficiency will guide the e-Govt-2024 implementation. Through these principles there will be:

- interoperability and accessibility to multiple choices with online service delivery;
- all-inclusive and compatible service delivery and utilisation;
- security, trust and confidence in government service delivery;
- economies of scale, and effective and efficient governance processes;
- partnership through collaboration and reliability;
- digital inclusion, accountability and responsiveness.

The National Broadband Strategy 2020–2024 and National Broadband Policy 2020–2024

These may also affect AI uptake and deployment as the policy documents provide a means to create/enable vital infrastructure to fuel the 4IR and the use of emerging technologies. The vision of the Policy is to transform The Gambia into a knowledge-based economy that thrives on accessible, secure and high-speed broadband in an open-access regime and a balanced broadband ecosystem. The Policy is premised on creating and establishing an economy and society that thrives on broadband, therefore positively affecting lives, governance and business processes, and with unlimited opportunities for all citizens.

Digital Health/E-Health

The Gambia's E-Health strategy is part of the broader health strategy, the National Health Policy 2021–2030. It governs digital health. The Gambia Public Health Act regulates health and the conduct of health professionals. Guidelines for Clinical Trials in Humans provided by the Medicines Control Agency regulate medical research. No legislation addresses software as a medical device. Medical devices are regulated by the Medicines Control Agency as stipulated by the Medicines and Related Products Act and the Medicines and Related Products Regulations.

Consumer Protection & ICT/E-Legislation

Consumer protection	• The Gambia Consumer Protection Act
ICT/E-Legislation	• Cybercrime Bill • Information and Communications Act

Data Protection Law

There are no data protection laws. However, with the Information and Communications Act, the Gambia Public Utilities Regulatory Authority, established under The Gambia Public Utilities Regulatory Authority Act, has the responsibility for regulating information and communications services, information and communications networks, associated facilities, and associated services.

However, the Information and Communications Act deals primarily with regulating IT service providers.

Information and Communications Act

Information and communications service providers are authorised to process the personal data of end users and subscribers, to the extent required and necessary:

- for their identification in order to draw up contracts for information and communications services;
- to define and amend the contents of these contracts;
- to monitor contractual performance, billing charges and fees as contracted;
- for enforcing any related claims.

Information and communications service providers are authorised to process personal data in connection with billing charges for information and communications services, to the extent required and necessary for calculating and billing charges, in particular the data relating to the date, duration and place of the service to which it pertains. In addition, information and communications service providers may also process the type of personal data which is technically essential for the provision of services.

Information and communications service providers must only use the type of information and communications apparatuses with sufficient facilities to ensure that personal data is processed only where it is absolutely necessary in terms of the provision of services and for the implementation of other objectives specified in the Act.

Information and communications service providers must delete any personal data from their records that is used for purposes other than those defined in the Act – immediately after gaining knowledge of unlawful data processing. The provision of information and communications services must not rely on the user providing consent for processing his or her personal data for purposes other than those defined in the Act.

Information and communications service providers must enable the end users to have access to information concerning the type of personal data the service provider is processing and the objectives – at any time before and during the use of the information and communications services.

Draft Data Protection and Privacy Policy and Strategy

The purpose of this Policy is to lay the foundations of an institutional and legal framework for data protection and privacy. The Policy applies to the processing of personal data in the private and public sectors, whether by automated or non-automated means and irrespective of the nationality or place of residence of the data subject. The Policy also seeks to establish a Gambian Data Protection Authority and impartial National Supervisory Authority. The principles in the Policy are based on international best practice considering the Malabo Convention and the modernised and most widely adopted globally – Convention 108+. These principles include: fair, transparent and lawful processing; specific legitimate purpose and purpose limitation; data minimisation, accuracy, data security and security breach notification; and accountability. Other important provisions consider the cross-border flow of personal data and the rights of the data subject. Vital for the deployment of AI systems is the right of the data subject not to be subject to a decision significantly affecting him or her based solely on automated processing of data – without having his or her views considered.

The processing of special categories of data, including personal health data and genetic data, are also treated. Processing may be undertaken only where appropriate safeguards are implemented. The safeguards must guard against risks that the processing of such data may present for the interests, rights and freedoms of the data subject – the risk of discrimination. Appropriate safeguards where the processing is carried out, include:

- the data subject's explicit consent;
- being under a professional secrecy obligation;
- in relation to a law covering the intended purpose and means of the processing or indicating the exceptional cases where processing such data would be permitted;
- involvement of a particular and qualified organisation or where processing is needed to protect the vital interests of the data subject or of another natural person.

Intellectual Property

Relevant Acts and their important definitions/provisions are:

Copyright Act

Computer programme means a set of instructions expressed in words, codes, schemes or in any other form, which can, when incorporated in a medium that the computer can read, cause a computer to perform or achieve a particular task or result.

Computer means an electronic or similar device with information-processing capabilities.

Literary work includes any of the following works or works similar to them: (i) encyclopaedias, dictionaries, directories, timetables, anthologies, databases or a compilation of data or other material, which constitutes intellectual creations; and (ii) computer programs.

Industrial Property Act

Classification of patents is the classification, grant and publication of patents and the maintenance of classified search files in accordance with the Strasbourg Agreement of 1971.

Summary and Analysis

While a number of ICT policy documents that support 4IR enablement have been produced, relevant provisions found in promulgated legislation take precedence over other regulatory/policy documents. The discussed policy documents are interoperable and do not supersede one another. These documents envision digital transformation across Gambia by leveraging ICT. Focus areas include strengthening ICT and broadband infrastructure, the provision of e-services and the development of a cybersecurity framework. Most of these instruments constitute new regulatory developments which are vital for ensuring that practical steps are taken to encourage the development and use of AI-based technologies. While several policy documents guide digital heath implementation, no specific legislation addresses software as a medical device.

There is no data protection legislation. However, the Information and Communications Act provides for the processing of personal data by IT service providers. In addition, the Draft Data Protection and Privacy Policy and Strategy aims to lay the foundation for a future data protection framework. Restrictions on the processing of personal data are particularly important for health research. Unfortunately, the Policy does not contain a provision that speaks to automated decision-making. The Gambia Consumer Protection Act provides safeguards against harmful technologies and provides for recall of such products where they are considered a risk to public health. ICT/E-legislation, such as the Cybercrime Bill and Information and Communications Act, and a consideration of intellectual property legislation, jurisprudence and soft law, may be essential for ensuring that these technologies are properly used.