UGANDA

ACRONYMS

4IR	Fourth Industrial Revolution
AFRO	Regional Office for Africa
AGL	Above ground level
AI	Artificial intelligence
CAA	Civil Aviation Authority
DPA	Data Protection Act
DRM	Disaster risk management
DPPA	Data Protection and Privacy Act
GDPR	General Data Protection Regulation (Europe)
ICT	Information and communication technology
IDSR	Integrated Disease Surveillance and Response
IP	Intellectual property
MoH	Minister of Health
MTA	Material transfer agreement
NDP	National Development Plan
NITA	National Information Technology Authority
PDPO	Personal Data Protection Office
PI	Principal investigator
RICA	Regulation of Interception of Communications Act
RPA	Remotely piloted aircraft
RPAS	Remotely Piloted Aircraft System
SDG	(United Nations) Sustainable Development Goals
TRIPS	Trade-Related Aspects of Intellectual Property Rights
UAS	Unmanned Aircraft System
UCC	Uganda Communications Commission
UNHRC	United Nations Human Rights Council
WHO	World Health Organization
WTO	World Trade Organization

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.

The general data protection legislation is the Data Protection and Privacy Act (DPPA) (2019).

Data Protection and Privacy Act

Obtaining consent

Prior consent of the data subject is required for the collection or processing of personal data. There are other ways to collect and process data but the data subject is allowed to object when such other means are used to stop the collection and processing of data. Where it is impossible to obtain the consent of the data subject, collection of the data from another source is allowed. No research exemption is provided for in the DPPA.

Collection and processing of specific types of personal data

The collection and processing of personal data relating to religious or philosophical beliefs, political opinion, sex life, financial information, health status or medical records of an individual is prohibited. This information may be collected or processed only if it is given freely and with the consent of the data subject.

Consent to further processing of personal data and retention of records

The data subject may also consent to the further processing of his or her personal data in a manner that is compatible with the purpose of collection. He or she may also consent to the retention of records of his or her personal data.

Consent and processing of personal data outside of Uganda

In relation to processing of personal data outside of Uganda, the consent of the data subject is required – in addition to adequacy measures.

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 well defined legislation or regulations governing human genomics research. The Constitution recognises cultural and customary values of people as those values are consistent with fundamental rights and freedoms, human dignity, democracy, and with the Constitution. It also establishes the Uganda Human Rights Commission whose functions include the establishment of continuing programmes of research, education and information to enhance respect for human rights.

Regulatory and Supporting Institutions

A number of institutions regulate and support compliance with general health research. These include (the):

- Human Heredity & Health in Africa
- Ministry of Health
- National Council of Science and Technology
- National Drug Authority
- Uganda Industrial Research Institute
- Uganda National Health Research Organization
- Uganda Virus Research Institute

Individual and Community Benefit Sharing

The approach to benefit sharing is as follows. Research and development, including scientific investigations involving humans, is to be done for the benefit of communities in Uganda. Benefits

arising from intellectual property rights must be shared in different ways and are to be pre-negotiated. Such benefits include: financial benefits, information, licensing, or transferring of technology or materials. The government must put in place policies and procedures on benefit sharing that are consistent with the law.

Benefits

(1) Tissue donation, removal and associated payment

No documented policies guide human organ/cell donation. However, The Uganda Human Organ Donation and Transplant Bill is likely to be enacted. The Bill seeks to establish a legal framework for the regulation of organ, cell and tissue donation and transplantation in Uganda. The Bill will apply to the donation and transplantation of human organs, tissues and cells, such as (the) kidneys, heart, blood, lungs, liver, pancreas, intestines, thymus, bone marrow, bone, tendon, ligaments, corneas, cells, skin, amniotic membrane, reproductive organs and other organs, cells and tissues related to the above organs. The Bill proposes a prohibition on monetary gain or payment for organs, tissues or cell donation and therefore criminalises trade in human organs, cells or tissues. However, donors can be compensated for expenses related to donation, including transport costs and injury incurred in the course of donation.

(2) Patenting

Patenting is allowed, but several inventions are not available for patenting. These relate to and include discoveries, scientific and mathematical theories, methods for treatment of the human or animal body by surgery or therapy, and diagnostic methods. The exclusions do not encompass methods of treatment that do not apply to the products used in treatment. The law is silent on 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, guidelines and policies are discussed below.

General Framework

Legislation

The Constitution of the Republic of Uganda

The Constitution introduces the right to privacy: no person must be subjected to interference in respect of the privacy of that person's home, correspondences, communication, or other property.

Data Protection and Privacy Act (DPPA)

The DPPA safeguards personal data collected and processed, and comprehensively provides for matters on data protection and privacy that were not addressed in the previous legal regime on data protection. This is in order to protect the privacy of the individual and personal data, and to regulate the collection and processing of personal data.

The DPPA provides that the regulatory body for data protection and privacy is the National Information Technology Authority. However, the DPPA provides that this must be done through the establishment of the Personal Data Protection Office (PDPO) which will be responsible for personal data protection under the Authority. It further provides that the Office, in performing its functions under the Act, must not be under the direction or control of any person or Authority.

Personal data

The DPPA defines personal data as information about a person from which the person can be identified that is recorded in any form and includes data that relates to the nationality, age or marital status of the person; the educational level or occupation of the person; as an identification number, symbol or other particulars assigned to a person; identity data or any other information which is in possession of, or is likely to come into the possession of, the data controller, and includes an expression of opinion about the individual.

There is no mention of address data or location data but it can be implied that such data, and consequently that geospatial data, must be treated as personal information where it may by used to identify an individual.

Special personal information

Although the DPPA further distinguishes between personal information and special personal information, it is doubtful that geospatial information can be considered to be special personal information because it is not listed, defined, or referred to in the definition of special personal information. Special personal information is defined in the DPPA and includes an individual's religious or philosophical beliefs, political opinion, sexual life, financial information, health status, or medical records. These considerations merit special attention by health researchers combining geospatial data with health data or medical records in such a way that individuals are identifiable. There is no research exemption in the DPPA and therefore all special personal information must be processed by researchers with consent from the individuals concerned. However, the DPPA expressly excludes information collected under the Uganda Bureau of Statistics Act from these additional protections.

Access to Information Act

This Act provides that every citizen has a right of access to information and records in the possession of the state or any public body, except where the release of the information is likely to prejudice the security or sovereignty of the state or interfere with the right to privacy of any other person. This may be the case if such geospatial data is to be linked with other sets of data that may identify and prejudice certain people.

The Act provides for the right of access to information pursuant to the Constitution, to prescribe the classes of information referred, the procedure for obtaining access to that information, and for related matters.

Anti-terrorism Act

This Act provides for the discretionary power of state officials to conduct surveillance without the need to obtain judicial authorisation. This in turn constitutes a legal ground for a breach of geospatial privacy.

The law criminalises perpetration, planning, and participation in any terrorist activities. In so doing, anyone who engages in or carries out any act of terrorism faces death upon conviction. The Anti-terrorism (Amendment) Act is currently in force.

Regulation of Interception of Communications Act (RICA)

RICA regulates the surveillance of communications by security services. Telecommunications service providers must enable interception of their services and store call-related information as directed by the Minister of Information and Communications Technology.

Lack of adequate safeguards

RICA lacks adequate safeguards to ensure protection of freedom of expression and the right to privacy. It gives the government unduly broad discretion to monitor and intercept electronic, telecommunications, and postal communications between individuals, groups and organisations. RICA's vague and excessively permissive basis for intercepting communications contravenes international standards, such as by sanctioning intrusions into the communications of individuals engaged in exercising their human rights.

Need for the revision of RICA

RICA defines the "national security of Uganda" as including "matters relating to the existence, independence or safety of the State". The United Nations Human Rights Council (UNHRC) has stated that "[a] law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution". The UN Special Rapporteur has raised concerns about the

amorphous concept of national security, noting that authorities can manipulate the concept to justify targeting vulnerable groups like human rights defenders, journalists or activists. According to the UN Special Rapporteur, the concept also allows for unnecessary secrecy about investigations or law-enforcement activities, therefore undermining the principles of transparency and accountability. RICA's definition of "national security of Uganda" is overly broad and open to interpretation, so violating the requirement that any restriction on the right to freedom of expression must be provided by law. The provision needs to be revised so that it is more precisely and narrowly defined. International norms state that any restrictions on the right to privacy must be prescribed by law, pursue a legitimate aim, and conform to the tests of necessity and proportionality. The test of necessity stipulates that any surveillance or interception activity "must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim". Therefore, such activities should be authorised only as a last resort. RICA falls short of these norms. According to RICA, a warrant for interception of communications will be issued to authorities if there are reasonable grounds for a designated judge to believe that:

> (a) an offence which may result in loss of life or threat to life has been or is being or will probably be committed;
> (b) an offence of drug trafficking or human trafficking has been or is being or will probably be committed;
> (c) the gathering of information concerning an actual threat to national security or to any national economic interest is necessary;
> (d) the gathering of information concerning a potential threat to public safety, national security or any national economic interest is necessary; or
> (e) there is a threat to the national interest involving the state's international relations or obligations.

Unmanned Aircraft System (UAS) Laws – general rules for flying drones in Uganda

The Ugandan agency responsible for drone safety, the Civil Aviation Authority (CAA), has not codified drone use regulations in Uganda. According to the CAA, drone operations are allowed in Uganda but are essentially limited to Ugandans, and are subject to CAA regulations.

Remotely Piloted Aircraft System (RPAS) operations will be categorised based on the risk posed by the type of operations, as follows:

- *category A operations*: basic operations which pose a low or minimal risk to the public, property and manned aviation;
- *category B operations*: specific operations which pose a medium risk to the public, property and manned aviation; and
- *category C operations*: complex, commercial or certified operations which pose a high risk to the safety of individuals, property and manned aviation.

Eligibility to own an RPAS is restricted to: citizens of or residents in Uganda aged 18 years and older; companies registered in Uganda; the Government of the Republic of Uganda.

The CAA requires the necessary security clearance and approval from the Office of the Chief of the Defence Forces.

An RPAS must not be operated at a height above 400 feet (120 metres) above ground level (AGL) and a lateral distance of 100 metres away from any person, vessel, vehicle or structure which is not under the control of the person in charge of the RPAS – except where approved by the Authority. An RPA must not be launched or recovered from any public or private property without consent. Any person conducting operations using an RPA fitted with cameras must operate in a responsible way that ensures the respect of privacy of other persons.

Guidelines and Policies

Third edition of the National Guidelines for Integrated Diseases Surveillance and Response in the African Region

The World Health Organization (WHO) Regional Office for Africa (AFRO), together with its technical partners, adopted a strategy for developing and implementing comprehensive public health surveillance and response systems in African countries, which was initially called Integrated

Disease Surveillance. However, to highlight the linkage between surveillance and response, the strategy was later renamed Integrated Disease Surveillance and Response (IDSR).

The Third Edition of IDSR highlights new methods of disease detection, reporting, and provision of real-time surveillance data using new technologies and platforms. The platforms include event-based disease surveillance, community-based surveillance, a one-health approach, cross-border surveillance, and electronic IDSR to improve disease surveillance in Uganda at all levels. The third edition is meant to upgrade the existing standards of the national disease surveillance system. It seeks to sustain the gains and progress made towards achieving an efficient surveillance system.

Historical review

The first edition of the IDSR technical guidelines was widely adopted by member states. Although progress towards a coordinated, integrated surveillance system has been mixed, almost every country in the region and their partners invested human and material resources in the process in an effort to build capacities for public health surveillance systems for early detection, confirmation, and response to public health threats, in order to prevent unnecessary illness, death and disability. The coming into force of the International Health Regulations, the emergence of new diseases, conditions, events, and the formulation of strategies for disaster risk management (DRM) drove the need to revise the first edition of the IDSR guidelines. There was also a need to address the increasing burden of non-communicable diseases. Furthermore, community-based surveillance for early detection, rapid confirmation, and response to public health threats had to be enhanced, while alignment with broader system-strengthening objectives was necessary. This led to the development of the second edition of the IDSR guidelines.

E-Health strategy/policy

The Uganda Communications Commission (UCC) undertook the e-Health project in addition to the Minister of Health (MoH) and a steering committee from both.

The Government of Uganda recognises e-Health as an enabling platform to improve healthcare delivery by allowing doctors to consult and diagnose remotely, access patients' medical information, provide district health information surveillance data, and facilitate research studies.

The national data transmission backbone and e-Government infrastructure project (NBI/EGI) connects Uganda to neighbouring countries and links major towns, cities and government ministries and departments, with 48 government departments and six universities currently connected. Improved internet bandwidth is seen as a major driver of voice and data communications that are required for e-Health services. Several studies conducted in developing countries, including Uganda, have demonstrated an increasing application of e-Health systems for healthcare delivery. The Government of Uganda recognises e-Health as a tool to improve health services' delivery to its citizens but the country's e-Health implementation status is unknown, and barriers and opportunities for sustainable e-Health implementation have not been documented.

According to Uganda's 2013 National e-Health Policy, most e-Health applications and products have been run in silos and are not interoperable or compatible, so preventing sharing of information and services. Several technology innovations have remained as pilots for life as they are not interoperable as a result of divergent platforms. Poor coordination and communication and a lack of proper e-Health implementation frameworks are also cited as major challenges to sustainable e-Health programmes. Uganda's National e-Health Policy also identifies the non-existence of e-Health standards and systems as challenges. There are no national guidelines for secure management of individuals' electronic health information and services, thereby placing personal data at risk. This may eventually be a barrier to the adoption of e-Health and the realisation of its benefits, such as enhancement of health information sharing and effective management of the health system. The Uganda Medical and Dental Practitioners Council, with an oversight function for legal and regulatory compliance, lacks competence in e-Health and has not provided ethical guidelines. e-Health innovations can reduce healthcare costs and enable access to better quality healthcare – provided there is adequate infrastructure.

Geospatial data can increase this value even more if it is integrated into the digital health system. However, all the difficulties experienced by this system also hamper the implementation and use of geospatial data. Development in this area is thus critical to inform developments in the area of geospatial data collection and use for public health emergencies.

Conclusion and Recommendations

Uganda has implemented a data protection law which can provide protection for individuals' personal data, but concerns remain about the extent to which unregulated state surveillance may infringe individual privacy rights.

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 DPPA, 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 DPPA and to begin to assist users in navigating it. It is not comprehensive, and users of the DPPA 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 personal data is governed by several laws and regulations, which must be carefully considered and complied with before researchers share data for research purposes. In Uganda, the Data Protection and Privacy Act (DPPA) is in place. It is a general data protection law that applies to the processing (i.e., use) of personal data in all sectors. While it is not a statute introduced specifically to regulate research, it applies to research that involves the

processing of personal data. It must be complied with when transferring personal data for research purposes.

Health Research Regulations Involving Human Participants 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). Uganda has not ratified the Malabo Convention.

The relevant national health legislation and guidelines are the:

- Access to Information Act
- Guidelines on Good Clinical Practice in the Conduct of Clinical Trials Involving Human Participants, 2019
- National Guidelines for Research Involving Humans as Research Participants, 2014
- National ICT Policy, 2014
- Public Health Act
- Uganda Health Research Organization Act

These laws, policies and guidelines set out the legal and ethical requirements that must be met for the conduct of research in Uganda and must be considered when effecting cross-border transfer of personal data. Furthermore, specifically for the cross-border sharing of data, a Research Ethics Committee must approve any cross-border data sharing, and there must be a local principal investigator and a MTA.

The Data Protection and Privacy Act

In addition to these legal and ethical requirements, the DPPA applies to the processing of all personal data, but unlike most data protection regulations there are no special provisions in place

for scientific research. The conditions set out in the DPPA 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 DPPA are discussed/defined below. This is not a thorough assessment of the DPPA 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 Data Protection and Privacy Act

	Legal definition	**Layman explanation**
Data subject	An individual from whom or in respect of whom personal information has been requested, collected, collated, processed or stored.	The person to whom the data relates.
Data controller	A person who alone, jointly with other persons or in common with other persons, or as a statutory duty, determines the purposes for and the manner in which personal data is processed or is to be processed.	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 processor	A person other than an employee of the data controller who processes the data on behalf of the data controller.	Someone who is not directly employed by the data controller but who processes personal data under the direction of the data controller. They may be a consultant, for example.
Authority	The National Information Technology Authority.	The independent body established to monitor and enforce compliance with the law.
Data Protection Officer	Not defined in the Act but provided for in the Act.	An individual in an organisation who is appointed to advise and to promote compliance with the law.

Recipient	A person to whom data is disclosed including an employee or agent of the data controller or the data processor to whom data is disclosed in the course of processing the data for the data controller. But this does not include a person to whom disclosure is made in respect of a particular inquiry pursuant to an enactment.	
Data collector	A person who collects personal data.	
Third party	A person other than the data subject, the data collector, data controller, or any data processor or other person authorised to process data for the data controller or data processor.	

Categories of Data Listed in the Data Protection and Privacy Act

	Legal definition	**Layman explanation**
Personal data	Information about a person from which the person can be identified, which is recorded in any form and includes data that relates to: (a) the nationality, age or marital status of the person; (b) the educational level or occupation of the person; (c) an identification number, symbol or other particulars assigned to a person; (d) identity data; or (e) other information which is in the possession of, or is likely to come into the possession of, the data controller and includes an expression of opinion about the individual.	Data/information about a particular person that can identify him or her.

Special personal data	Not defined. However, the DPPA provides that special personal data relates to religious or philosophical beliefs, political opinion, sexual life, financial information, health status or the medical records of an individual	Personal data about a particular person that is particularly sensitive, such as health data and genetic data, and which receives additional legal protection.

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 come under the definition of personal data, data protection law does not apply. The DPPA applies specifically to the processing of "personal data". The DPPA defines personal data as "information about a person from which the person can be identified". Therefore, if the data is not personally identifiable, such as where it has been anonymised, it would not fall under the application of the DPPA. The terms 'de-identified' or 'anonymised' are not used in the DPPA.

To determine whether data to be shared is anonymised, it is important to make an assessment, which can be challenging. There is no guidance from the Authority on this point, but the data controller may wish to follow the guidance set out to be followed under the GDPR on how to make an assessment to determine whether data is anonymous, including guidance on anonymisation techniques.

There is some debate about from whose perspective the data must be considered anonymised.

There are two possibilities, and with two different possible tests:

(1) Is there anyone in the world who can identify the data subject from the data? (This is an objective test that is context-agnostic, and so considers the data in the context of anyone in the world.)
(2) Can a specific holder of the data identify the data subject from the data? (This is an objective test that considers the data specifically in the hands of the recipient. This means that data can be non-personal in one holder's hands, but personal in another holder's hands.)

Applying the first test would mean that if Data Controller A sends pseudonymised data (i.e., Data Controller A has the necessary information to identify the people in the dataset) to Controller B, the dataset would not be anonymous.

The context-specific test would mean that if Data Controller A sends pseudonymised data (i.e., Data Controller A has the necessary information to identify the people in the dataset) to Controller B, the dataset *may* be anonymous in the hands of Data Controller B. A test would be needed to determine whether the dataset is anonymous in the hands of Data Controller B.

In the absence of direction from the Office on a test, the data controller must decide. In making this decision, general points may be worth bearing in mind (many of which come from guidance related to anonymisation under the GDPR):

- An assessment must be made on a case-by-case basis, considering the particular context.
- The anonymisation must be irreversible.
- The assessment is made based on the current state of the art. As technology progresses, data that was once deemed to be anonymous may become personal data and therefore fall under data protection regulations.
- Consider all means of identification that could be used by a person, for example, available datasets.
- Consider objective factors that are *reasonably likely* to be used, such as technology, resources and time, to identify.
- It is possible to follow the GDPR test which states that if an individual cannot be singled out, or identifiers cannot be linked to make a person identifiable, or it is impossible to infer a link between two pieces of information in a dataset, then the data is anonymous.
- Genetic data is not mentioned in the Act, but health data is. Genetic data is generally considered to be special personal data, which has a higher level of protection.
- There is ongoing debate about whether genomic datasets can ever be rendered truly anonymised, particularly as genetic data is an identifier. In considering whether a genomic

dataset can be considered anonymised, context matters – the objective factors associated with the data.

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

1. *Accountability: Be accountable to the data subject for data collected, processed, held or used.* The data controller, data processor or data collector are responsible for, and must be able to demonstrate compliance with, the principles mentioned above. Keep a record of data processing activities, measures introduced to protect the data, as well as of any risk assessments made. These can be used to demonstrate compliance in the event of a breach.
2. *Collect and process data fairly and lawfully:* Personal data must be processed lawfully, fairly, and transparently in relation to the data subject. Lawful means that there must be a legal basis for the processing of the personal data as set out in law.
3. *Data minimisation: Collect, process or hold adequate, relevant and not excessive or unnecessary personal data.* Only the data that is necessary for the specific purpose should be collected and processed. It is essential that only the minimal amount of data that is required to achieve the objectives of the data processing is used.
4. *Storage limitation: The data collector, data processor or data controller or any person who collects, processes, holds or uses personal data should retain it for the period authorised or for which it is required.* Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Once the objective of the processing has been achieved, the data should be deleted. Data that is rendered anonymous does not fall under data protection law. However, to anonymise the data, there must still be a lawful basis to do so.
5. *Data quality: Ensure quality of information collected, processed, used or held:* 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. *Openness: Ensure transparency and participation of the data subject in the collection, processing, use and holding of personal data:* Personal data must be processed lawfully, fairly, and transparently in relation to the data subject. Lawful means that there must be a

legal basis for the processing of the personal data as set on in the DPPA. The processing of sensitive personal data is generally permitted unless it falls within one of the grounds as set out in the DPPA.

7. *Observe security safeguards in respect of the data:* Personal data should be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Both organisational and technical measures must be put in place to secure the data.

Data Subject Rights Under the Data Protection and Privacy Act

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

(1) *Right to access personal information:* A data subject who provides proof of identity may request a data controller to confirm whether the data controller holds personal data about the data subject, give a description of the personal data which is held by the data controller, and provide the identity of a third party or a category of a third party who has or has had access to information.

(2) *Right to prevent processing of personal data:* A data subject must at any time, by notice in writing to a data controller or data processor, require the data controller or data processor to stop processing personal data which causes or is likely to cause unwarranted substantial damage or distress to the data subject. In addition, a data controller must within 14 days after receipt of a notice inform the data subject in writing that the data controller has complied or intends to comply with the notice of the data subject, or give the reasons for non-compliance.

(3) *Right to prevent processing of data for direct marketing:* A data subject may by notice in writing to a data controller, require the data controller to stop processing his or her personal data for purposes of direct marketing. In addition, a data controller must within 14 days after receipt of notice inform the data subject in writing that the data controller has complied or intends to comply with the notice of the data subject, or give the reasons for non-compliance.

(4) *Rights in relation to automated decision-making:* A data subject may by notice in writing to a data controller require the data controller to ensure that any decision taken by or on behalf of

the data controller which significantly affects that data subject is not based solely on the processing by automatic means of personal data in respect of the data subject.

(5) *Right to rectification, blocking, erasure and destruction of personal data:* Where the Authority is satisfied about the complaint of a data subject that personal data on that data subject is inaccurate, the Authority may order the data controller to rectify, update, block, erase or destroy the data.

Cross-Border Data Sharing

Each of the above provisions applies to any research that uses personal data. Data protection law also has additional provisions 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.

While cross-border sharing is not defined in data protection law, the laws on cross-border data sharing clearly apply to data sent to a data controller in another country. It *could* also include when a researcher outside of the country accesses the personal data in the country. It *could* also include putting data onto a cloud where the server is not hosted in the country. Whether it does or not is not yet settled law.

In addition, there must be a ground under which transfer can occur. In terms of the DPPA, the legal bases for transferring personal (including health) data outside Uganda are:

(1) The country in which the data is processed or stored has adequate measures in place for the protection of personal data that are at least equivalent to the protection provided for by the DPPA; or

(2) The data subject has consented.

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

No specific AI legislation has been promulgated in Uganda. There is also no particular legislative provision that addresses AI-related issues including predictive algorithms. Furthermore, there is no technological provision or industry- or sector-specific guidance in place. It is therefore necessary to consider the legal landscape associated with 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; (3) Data protection law; and (5) Intellectual property.

AI Strategy

The most significant contribution to AI regulation is:

National 4IR Strategy, 2020

This addresses opportunities to become a continental 4IR hub in Africa that enables a smart and connected Ugandan society. The Strategy is aimed at developing Uganda into a technology and innovation hub by leveraging 4IR technologies to drive productivity, generate jobs and a knowledge-based society, establish smart cities and resource management systems, support national security, performance and service delivery, and increase research and innovation.

The Strategy has a three-part framework:

1. Identifying key opportunity zones such as increased agricultural productivity, human capital development, urbanisation and governance and economic opportunity through better supply chain management systems, and increased access to e-services.

2. Underscoring critical 4IR enablers such as widespread connectivity, agile governance, upskilling the population, provision of government e-services, and resource mobilisation.
3. Providing delivery mechanisms such as those regarding government and funding coordination and ecosystem facilitation. These provide for practical implementation channels to ensure the realisation of the strategy objectives.

Digital Health/e-Health

The Uganda National eHealth Strategy 2017–2021 guides digital health initiatives. There are however no standalone laws that apply to e-Health or health data. The National Drug Policy and Authority Act of the laws of Uganda and The National Drug Authority Draft Guideline for Registration of Medical Devices for Human Use in Uganda regulate medical devices in Uganda.

The National Drug Authority is the regulatory authority for medical devices. The Uganda Standards and International Organisation for Standardisation provides complementary guidance for medical devices. The National Drug Authority Draft Guideline for Registration of Medical Devices for Human Use in Uganda includes software in the definition of a medical device. However, there is no specific legislation for AI medical devices used in healthcare.

Consumer Protection and ICT/E-Legislation

Consumer Protection	There is a fragmented consumer protection regulatory framework Sale of Goods and Supply of Services Act There is no general consumer protection law. However, the Electronic Transactions Act offers a degree of protection to consumers involved in e-transactions. It also requires that an opportunity be provided to withdraw from the electronic transaction before it is concluded and requires a person offering services electronically to use a secure and technologically accepted payment system. The Act makes it unlawful for an electronic medium to contain a provision that purports to exclude the rights of consumers as provided for under the Act.

ICT/E-Legislation	Regulation of Interception of Communications Act Electronic Transactions Act and Electronic Transactions Regulations National Information Technology Authority Act; National Information Technology Authority; Uganda (Certification of Provider of Information Technology Products and Services) Regulations; National Information Technology Authority, Uganda (EGovernment) Regulations Computer Misuse Act Uganda Communications Act and Uganda Communications Amendment Act; Uganda Communications (Intelligent Network Monitoring System) Regulations; Uganda Communications (Content) Regulations; Uganda Communications (Universal Service) Regulations; Uganda Communications (Text and Multimedia Messaging) Regulations; Uganda Communications (Quality of Service) Regulations; Uganda Communications (Interconnection and Access) Regulations; Uganda Communications (Equipment Type Approval) Regulations; Uganda Communications (Consumer Protection) Regulations; Uganda Communications (Competition) Regulations The Ugandan Electronic Transactions Act, the Computer Misuse Act and the Electronic Signatures Act are the backbone of the e-legislative framework.

Data Protection Law

While no AI-specific legislation has been developed, data protection law will heavily influence the uptake of AI systems in the country. The primary legislation governing data protection is the Data Protection and Privacy Act which imposes restrictions on the processing of sensitive (health/genomic) data and prohibits automated decision-making.

Data Protection and Privacy Act

The DPPA provides that a data subject may require that the data controller ensure that any decision taken is not based solely on the automated processing of personal data. Where a decision that significantly affects the data subject is based solely on such data, the data controller is required to notify the data subject as soon as possible. After this, the data subject may require that the data controller reconsider the decision within 21 days. Upon receipt of written notice, the data controller must, within 21 days, inform the data subject in writing of the steps taken to comply. Where the data subject is not satisfied with the decision of the data controller, he/she can complain in writing to the Authority, within 14 days. Where the Authority agrees with the complaint, it must order the

data controller to comply within 7 days. This does not apply to decisions made in relation to a contract or for a purpose authorised or required by law.

Personal Data Protection Office

The Personal Data Protection Office is Uganda's independent data protection authority. It is established as an independent office under the National Information Technology Authority (NITA-U). NITA-U is responsible for overseeing the implementation and enforcement of the DPPA.

Intellectual Property

The following statutes and policy are relevant:

The Constitution of Uganda

The Constitution provides for the right to own property but it does not explicitly provide for the protection of IP rights. Nonetheless, a number of national and sectoral polices, strategies and plans address IP issues, which have laid the foundations for innovation and creativity.

The National Intellectual Property Policy

This Policy, through IP, intends to support efforts in achieving the objectives of Uganda Vision 2040, the Second National Development Plan (NDPII, 2015/16-2020/2021), and the United Nations Sustainable Development Goals (SDGs).

The Copyright and Neighbouring Rights Act

The Act has extended eligibility for copyright protection to computer programs and derivative work, which by selection and arrangement of its content constitute original work, illustrations, maps, plans, sketches and three-dimensional works relative to geography, topography, architecture or science, choreographic works, and pantomimes. This is in addition to those previously protected under the repealed legislation, including literary, musical, and artistic works, cinematography films, gramophone records, and broadcasts. In order for such works to be eligible for copyright protection they must be original and the product of the independent efforts of the author.

The Patents Act

The law defines an invention as a solution to a specific problem in the field of technology, which may be or may relate to a product or a process. The following are not regarded as inventions and are excluded from patent protection:

(a) discoveries, scientific theories and mathematical schemes;
(b) schemes, rules or methods for doing business, performing purely mental acts, or playing games;
(c) diagnostic, therapeutic and surgical methods for the treatment of humans or animals;
(d) mere presentation of information;
(e) plants and animals other than microorganisms, and biological processes for the production of plants or animals other than biological and microbiological processes;
(f) pharmaceutical products and test data until 1 January 2016 or other period granted to least-developed countries by the Council administering the TRIPS Agreement under the WTO;
(g) natural substances apart from the processes of isolating those natural substances from their original environment;
(h) the human body and all its elements – wholly or partly.

In line with the TRIPS Agreement, the Industrial Property Act provides that an invention is patentable if it is new, involves an inventive step, and is industrially applicable.

Summary and Analysis

The above policy documents and guidelines are interoperable and do not supersede one another, although relevant provisions in promulgated legislation take precedence over regulatory/policy documents. New regulatory developments such as the National 4IR Strategy, 2020 are vital for ensuring practicable steps to encourage the development and use of AI-based technologies. While software is included in the definition of medical devices, there is no specific legislation for AI medical devices used in healthcare.

Uganda's Data Protection and Privacy Act governs the processing of personal data. Particularly important are restrictions on the processing of sensitive (health/genomic) data and the prohibition on automated decision-making. AI technologies may receive some protection under the Sale of Goods Act as software is included in the provided definition of 'goods'. In addition, ICT/E-legislation, such as the Ugandan Electronic Transactions Act and the Computer Misuse Act and a consideration of IP legislation, jurisprudence and soft law may be essential for ensuring that these technologies are used properly.