TANZANIA

ACRONYMS

4IR	Fourth Industrial Revolution
AI	Artificial intelligence
ARIPO	African Regional Intellectual Property Organization
COSTECH	Commission for Science and Technology
CRA	Communication Regulatory Authority
CST	Copyright Society of Tanzania
EPOCA	Electronic and Postal Communications Act
GDPR	General Data Protection Regulation (Europe)
GIS	Geographical information system
ICT	Information and communication technology
IP	Intellectual property
IPR	Intellectual property rights
NIMR	National Institute for Medical Research
PDPA	Personal Data Protection Act
PI	Principal investigator
STIPRO	Science, Technology and Innovation Policy Research Organization
TCRA	Tanzania Communications and Regulatory Authority
TISS	Tanzania Intelligence & Security Service
TISSA	Tanzania Intelligence & Security Services Act
TSHG	Tanzania Society of Human Genetics
UHC	Universal health care
WIPO	World Intellectual Property 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 data protection legislation is the Personal Data Protection Act (PDPA) (2022).

The Personal Data Protection Act

In the PDPA, consent is defined in a manner consistent with specific informed consent requirements, and health data is classified as sensitive personal data.

Consent and personal data and its processing

Consent may be required during the collection of personal data for a specific purpose. Further processing of the data may also require the consent of the data subject.

Research exemption

There is a research exemption provision in the PDPA.

Consent for transfer of data outside of Tanzania

For transfer of data outside of Tanzania, consent of the data subject is required.

INDIVIDUAL AND COMMUNITY RIGHTS IN GENOMIC DATA

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

Many rights relevant to human genomics research are protected. The law provides for the right to equality, and subjects civic rights, duties and interests of every person and community to the law and these are to be determined by courts of law or other state agencies. These rights are pronounced in the Constitution and are provided for in legislation, regulations and policy guidelines.

Regulatory and Supporting Institutions

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

- BMC Medical Ethics
- Clinical Research SGS Tanzania
- Ministry of Health
- National Institute for Medical Research (NIMR)
- OneTrust Data Guidance
- Science, Technology and Innovation Policy Research Organization (STIPRO)
- Tanzania Commission for Science and Technology
- Tanzania Medicines and Medical Devices Authority
- Tanzania Society of Human Genetics (TSHG).

Individual and Community Benefit Sharing

The approach to benefit sharing is as follows. Although reasons for the involvement of research participants in research activities may be different, the benefits to the community where the research has been conducted must outweigh the risks associated with the research project. The law does not state much about individual and community benefit sharing.

Benefits

(1) Tissue donation, removal and associated payment

There is no comprehensive legal regulatory framework for human organ and tissue donation and transplantation. However, some regulations and policies govern research on human participants. For instance, where a research participant consents to participate in research, such a participant must be adequately informed of the aims, methods, anticipated benefits and potential hazards and discomforts of the research. In addition, such a research subject has to be adequately provided with compensation as far as ethical regulations are concerned. Therefore, research subjects who suffer injury or illness as a result of participating in a research project are legally entitled to compensation only on showing evidence of negligence on the part of the investigator, the host institution, the sponsor of the research and/or a respective staff.

There is no payment or reward for donation of blood or a body organ, as donation must be voluntary and non-remunerated.

(2) Patenting

Patenting is allowed in Tanzania. However, several inventions are not available for patenting. These include discoveries, scientific and mathematical theories, methods for the treatment of the human or animal body by surgery or therapy, as well as diagnostic methods. While a patent is meant for industrial application and commercial use, such industrial application and commercial use is prohibited in cases of scientific research.

The law does not mention patents relating to human genetic material.

GEOSPATIAL DATA FOR PUBLIC HEALTH SURVEILLANCE

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

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

General Framework

Legislation

The Personal Data Protection Act (PDPA)

It is important to note that in terms of the definition of sensitive personal data, genetic data and data related to children are only considered sensitive personal data if they are processed for what they reveal about health or race. This makes the category of sensitive data more restrictive. There is a wider scope to process health data under the PDPA.

Definition of personal data

According to the PDPA, personal data means data about an identifiable person that is recorded in any form, including:

a) personal data relating to the race, national or ethnic origin, religion, age or marital status of the individual;
b) personal data relating to educational, medical, criminal or employment history;
c) any identifying number, symbol or other particular assigned to the individual;
d) the address, fingerprints or blood type of the individual;
e) the name of the individual appearing on the personal data of another person relating to the individual or where the disclosure of the name itself would reveal personal data about the individual;

f) correspondence sent to a data controller by the data subject that is explicitly or implicitly private or confidential, and replies to such correspondence that would reveal the contents of the original correspondence, and the views or opinions of any other person about the data subject.

Definition of sensitive personal data

Sensitive personal data includes:

a) genetic data, data related to children, data related to offences, financial transactions of the individual, security measures or biometric data;
b) if they are processed for what they reveal, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, affiliation, trade-union membership, gender and data concerning health or sex life;
c) any personal data otherwise considered under the laws of the country as presenting a major risk to the rights and interests of the data subject.

The PDPA also requires that persons must be registered as a data controller in terms of the Act.

The Act relates to (a) any collection and processing of personal data performed wholly or partly by manual or automated means; (b) the processing of personal data carried out in the performance of the activities of a data controller based in Tanzania or in a territory where the laws of Tanzania apply by virtue of international public law; and (c) the processing of personal data by a data controller or data processor who is not based in Tanzania, if the processing of the personal data is in Tanzania and such processing is not for the purposes of mere transit of personal data through Tanzania to another country.

A data controller must collect personal data if (a) the personal data is collected for a lawful purpose related to a function of the data controller; and (b) the collection of the data is necessary or incidental or directly related to the lawful purpose. A data controller must not collect personal data unlawfully and must collect personal data directly from the data subject.

Before collecting data, a data controller must ensure that the data subject is aware of (a) the purposes for which the personal data is collected; (b) the fact that collection of the personal data is for authorised purposes; and (c) any intended recipients of the personal data.

To the extent that health data is discovered as personal sensitive data, there is a prohibition on processing it without prior consent, which the data subject can withdraw at any time.

Consent provisions

The above does not apply to research. Although there is an intention to authorise scientific research exemption from the requirement to get individual consent, unless and until the Commission sets out those guidelines it is impossible to comply with them to align with this provision. Currently, under the PDPA, the processing of health data requires consent. Consent is not necessary where the processing

a) is necessary for compliance with other written laws;
b) is necessary to protect the vital interests of the data subject or of another person, where the data subject is incapable of giving his/her consent or is not represented by his/her legal representative;
c) is necessary for the institution, trial or defence of legal claims;
d) relates to personal data which has apparently been made public by the data subject;
e) is necessary for scientific research and the Commission has, by special guidelines, specified the circumstances under which such processing may be undertaken; or
f) is necessary for medical reasons in the interest of the data subject, and the sensitive personal data concerned is processed under the supervision of a health professional in accordance with the law governing such healthcare services.

Electronic and Postal Communications Act (EPOCA)

The Act requires that all subscriber information and the subscriber database be kept within the Authority. These provisions potentially create room for easy monitoring and surveillance of individuals' communications, thereby violating their privacy. EPOCA provides that every application services' licensee be required to submit to the Authority a list containing its

subscriber's information once a month. The Authority must issue guidelines on details of subscribers' information to be submitted.

EPOCA requires the registration of SIM card owners. It provides that every person who owns or intends to use a detachable SIM card or built-in SIM card mobile telephone is obliged to register it. It also provides that:

> Any person who sells or, in any other manner provides a detachable SIM card or built-in SIM card mobile telephone to any potential subscriber shall:
> (a) where the potential subscriber is a natural person, obtain and fill in a form which contains the following information-
> (i) the full name of the potential subscriber;
> (ii) identity card number or any other document which proves the identity of the potential subscriber; and
> (iii) residential and business or registered physical address, whichever is applicable.

EPOCA mandates the Communication Regulatory Authority (CRA) to maintain a database of all subscribers' information. Service providers are required to submit all subscriber information to the CRA every month. It has been argued that mandatory SIM card registration eradicates the potential for anonymity of communications, enables location-tracking and simplifies communications surveillance and interception – thereby interfering with the right to privacy. EPOCA prohibits the interception of any communication, disclosure of the content of communication, or use of the content of intercepted communications without lawful authority. It provides a penalty of five million Tanzanian shillings or to imprisonment for a term not less than 12 months, or both.

Tanzania Intelligence & Security Services Act (TISSA)

TISSA can authorise the interception of any communication on the basis of national security. TISSA empowers the Tanzania Intelligence & Security Service (TISS) to collect, analyse, and retain information and intelligence on activities that may on reasonable grounds be suspected of constituting a threat to the security of the country. However, TISSA is barred from instituting surveillance of any person or category of persons by reason only of their involvement in lawful

protest, or dissent in respect of any matter affecting the Constitution, laws, or the Government of Tanzania. This means that surveillance can be instituted for other grounds such as national security.

Cybercrimes Act

In terms of the Act, the Minister can prescribe procedures for service providers to provide competent authorities with some information – although the procedures have not been developed. There are concerns about increased surveillance of social media platforms by law-enforcement agencies (CIPESA 'State of Internet Freedom in Africa 2018 Privacy and personal data protection in Tanzania: Challenges and trends').

According to the Cybercrimes Act:

> (1) When providing services in accordance with the provisions of this Part, a service provider shall not-
> (a) monitor the data that the service provider transmits or stores; or
> (b) actively seek facts or circumstances indicating an unlawful activity.
> (2) The Minister may prescribe procedures for service providers to-
> (a) inform the competent authority of alleged illegal activities undertaken or information provided by recipients of their service; and
> (b) avail competent authorities, at their request, with information enabling the identification of recipients of their service, which may include geospatial data.
> (3) A service provider shall not be liable for disclosure by a third party of data lawfully made available to the third party upon proving that-
> (a) the third party acted without the knowledge of the service provider; or
> (b) the service provider exercised due care and skill to prevent the disclosure of such data.
> (4) Where a service provider has knowledge of illegal information or activity, he shall-
> (a) remove the information in the computer system within the service provider's control;
> (b) suspend or terminate services in respect of that information or activity; and

(c) notify the appropriate law-enforcement authority of the illegal activity or information, relevant facts, and the identity of the person for whom the service provider is supplying services in respect of the information.

The case of *Jamii Media Company Ltd v The Attorney General* (2017) involved the limitations placed on privacy rights of the Media Company's platform users. They claimed that transferring the personal information to the police when they requested access infringed their privacy. However, the court decided that this limitation was necessary and was within the permissible limits, such as law enforcement purposes, and that a breach of privacy is sometimes justified. The Cybercrimes Act was reasonable in giving police that power. The court's approach to this matter could be applied to geospatial data collection and transfer. This means that under exceptional circumstances, data transfer could be allowed without consent, for example.

Regulations, Guidelines and Policies

The Electronic and Postal Communications (Online Content) Regulations, 2020

The regulations have been widely criticised for having an adverse impact on the right to privacy. For instance, Regulation 9 requires online content providers to have surveillance systems in place to identify the source of information or content, while Regulation 13 provides for the installation of cameras in internet cafes and the storage of recorded images for at least 12 months. This also relates to geospatial data to the extent that it can confirm the physical presence of a person at a particular place and time which, in the context of abortion services, for example, may breach the privacy and related rights of people.

Guideline for GIS Application in Local Government Authorities, 2022

Given that data processing was largely manual in the past, there is a need to provide guidelines for automated processing of spatial data using GIS. The Guideline aims to make better use of the spatial information held by public authorities. This will be done by using GIS to make better decisions about the data, such as it may be used to ascertain the presence of populations at particular places and how they may be influenced by infectious diseases and their spread, or how

many and where to best deploy medical services and personnel to attend to the medical needs of these people.

Health Sector Strategic Plan July 2021–June 2026

The core functions of public health laboratories will be strengthened, including disease prevention, control and surveillance, reference and specialised testing, environmental health and protection testing, food safety testing, laboratory regulations, and policy development. The plan may be used to ascertain the presence of populations at particular places and how they are influenced by infectious diseases and their spread, or how, how many and where to best deploy medical services and personnel to attend to the medical needs of these people.

The National Health Policy, 2017

Objectives include delivering a package of essential services in communities and health facilities and equitable access to services by focusing on geographic areas with higher disease burdens and on vulnerable groups in the population with higher risks, among other things.

Surveillance is used for a number of reasons in relation to healthcare, such as diagnostic services and dealing with epidemics.

'Fit-for purpose' approaches and technologies such as the discipline of One Health, use of participatory epidemiology, disease surveillance, and mobile technologies offer opportunities for optimal use of limited resources to improve early detection, diagnosis, and response to disease events and consequently reduced impact of such diseases on animals and human populations. Community-based surveillance systems have however not been effectively incorporated into the national systems for early detection of public health events. Also, there is limited coordination and collaboration between the health sector and other sectors and limited participation of non-state actors in addressing emerging and re-emerging diseases.

The health and social welfare sector will improve and integrate systems including data collection tools, planning, budgeting, and reporting tools across government. The Ministry will work with all partners to ensure that the *electronically geocoded* health facility registry is efficiently and

effectively functioning. The Ministry will coordinate *population-based data systems* and continue to use surveys and sample-based sentinel sites to provide nationally representative evidence on community health status and vital statistics. Using a coordinated approach collaboration with the agency responsible for birth and death registration will be important to determine the readiness of this source for generating vital registration data. The sector will improve data collection and analysis with regard to nutrition, and will link information on food security to data concerning malnutrition. This will enable the identification of weak spots and vulnerable areas.

National ICT Policy, 2016

ICT has contributed to improvements in public and private sector service delivery. These include healthcare, formal and informal education, and various e-services contributing to the manifestation of e-government.

This Policy further sets out that the government must ensure that a digital dividend is dedicated to the government for bridging the digital divide that is necessary for e-service delivery, specifically in rural areas. This is important because if electronically obtained data is used to control and manage public health emergencies, the government must ensure that all citizens can be captured by this system and that nobody is left behind digitally.

Conclusion and Recommendations

In terms of the Personal Data Protection Act, a person's address is considered to be personal data which can be used to identify a person, especially in combination with other personal data points such as health data. Accordingly, geospatial data falls within the scope of the PDPA and must be regulated as personal data.

One of the main aims of the National Health Policy of 2017 is the delivery of essential services to communities and health facilities to ensure equitable access to health services by focusing on geographical areas with higher disease burdens, including vulnerable groups in the population with higher risks. For this purpose, Tanzania will increasingly use surveillance technologies which will affect the privacy rights of individuals in the context of geospatial data. This type of surveillance

and its impact on the privacy rights of individuals must be weighed against the public health interest of the country's citizens, especially during pandemics or epidemics. However, regardless of the fact that mobile phone usage has exploded in recent years in sub-Saharan Africa, including Tanzania, accurate digital maps and time estimates for travel are not always available, which severely hampers the supply and transit of medical goods, resulting in serious gaps in healthcare for rural people.

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 PDPA, 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 PDPA and to begin to assist users in navigating the PDPA. It is not comprehensive, and users of this Act 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 Tanzania, the Personal Data Protection Act (PDPA) is in force. 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 law introduced specifically to regulate research, it applies to research that involves the processing of

personal data. It is only one of several laws that 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. However, Tanzania has not yet ratified the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention).

The relevant national legislation is the:

- Constitution of the United Republic of Tanzania
- Guidelines of Ethics for Health Research In Tanzania
- Human DNA Regulations Act
- Tanzania Commission for Science and Technology Act
- Tanzania Food, Drugs and Cosmetics Act
- Tanzania National Scientific Research Council (Amendment) Act
- Tanzania National Scientific Research Council Act

These laws and guidelines set out the legal and ethical requirements that must be met for the conduct of research in Tanzania and must be considered when effecting cross-border transfer of personal data. It is an offence to send samples for human DNA analysis abroad without the permission of the Office of the Regulator of Human DNA Services. Moreover, the National Institute for Medical Research (NIMR) must approve all research that involves foreign researchers or collaborators. A contract agreement is recommended for all research involving external researchers.[1]

Personal Data Protection Act

[1] para 8.9. http://www.cohred.org/wp-content/uploads/2011/05/ETHICS-GUIDELINE-2009.pdf.

In addition to these legal and ethical requirements, the Personal Data Protection Act (PDPA) applies to the processing of all personal data, with special provisions in place that deal with the processing of personal data for research purposes. Two regulations related to this Act are also important: the Personal Data Protection (Personal Data Collection and Processing) Regulations and the Personal Data Protection (Complaints Settlement Procedures) Regulations.

For research, the PDPA exempts the requirement of prior written consent for processing of sensitive personal data if the processing is necessary for scientific research and the Commission has, by special guidelines, specified the circumstances under which such processing may be carried out. This means that the consent requirement is not applicable in relation to scientific research but a special guideline must be put in place describing the circumstances applicable.

Extra conditions must be met prior to the transfer of personal data across borders.

Techno-legal terms used in the PDPA are discussed below. This is not a thorough assessment of the PDPA 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 Personal Data Protection Act

	Legal definition	**Layman explanation**
Data subject	The subject of personal data which is processed under the PDPA.	The person to whom the data relates.
Data controller	A natural person, legal person or public body which alone or jointly with others determines the purpose and means of processing of personal data; and where the purpose and means of processing are determined by law, "data controller" is the natural person, legal person or public body designated as such by that law and it includes his/her representative.	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 natural person, legal person or public body which processes personal data for and on behalf of the data controller and under the data controller's instruction, except for the persons who, under the direct authority of the data controller, are authorised to process the data, and it includes his/her representative.	Someone who is not directly employed by the data controller but who processes personal data under the direction of the data controller. He/she may be a consultant, for example.
Data Protection Commission		The independent body established to monitor and enforce compliance with the law
Data Protection Officer	An individual appointed by the data controller or data processor who is charged with ensuring compliance with the obligations provided for in the PDPA.	An individual in an organisation who is appointed to advise and promote compliance with the law.
Health professional	A person providing healthcare services and who is recognised as such by the relevant law.	
Director General	The Director General of the Commission, who is appointed under the PDPA.	
Recipient	A natural person, legal person, public body or any other person who receives personal data from a data controller.	

Categories of Data Listed in the Personal Data Protection Act

	Legal definition	**Layman explanation**
Personal data	Data about an identifiable person that is recorded in any form, including: (a) personal data relating to the race, national or ethnic origin, religion, age or marital status of the individual; (b) personal data relating to the education, medical, criminal or	Data about a particular person that can identify him or her.

	employment history; (c) any identifying number, symbol or other particular assigned to the individual; (d) the address, fingerprints or blood type of the individual; (e) the name of the individual appearing on personal data of another person relating to the individual or where the disclosure of the name itself would reveal personal data about the individual; (f) correspondence sent to a data controller by the data subject that is explicitly or implicitly private or confidential, and replies to such correspondence that would reveal the contents of the original correspondence and the views or opinions of any other person about the data subject.	
Sensitive personal data	Sensitive personal data includes: (a) genetic data, data related to children, offences, financial transactions of the individual, security measures or biometric data; (b) if it is processed for what it reveals, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, affiliation, trade-union membership, gender, and data concerning health or information on sex life; and (c) any personal data otherwise considered under the laws of the country as presenting a major risk to the rights and interests of the data subject.	Personal data about a particular person that is sensitive, such as health data and genetic data, and which receives additional legal protection.
Genetic data	Any personal data stemming from a DNA analysis.	Data that is derived from the analysis of human DNA.

Anonymous data	Not defined.	Data from which it is no longer possible to identify a person. It must be impossible to re-identify the person. Data protection law does not apply to anonymised data.

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 Personal Data Protection Act applies to "the processing of personal data".

The PDPA does not mention anonymised data. However, it allows the data controller to use personal data for purposes other than for which it was collected where it is "in a form in which the data subject is not identified" and for statistical or research purposes, as long as it is not published in a form that could reasonably be expected to identify the data subject. The test in the PDPA is whether it may reasonably be expected that the data subject could be identified and so the context suggests that the PDPA is not referring to anonymisation but to something less absolute.

Although the Personal Data Protection (Personal Data Collection and Processing) Regulations mention anonymisation, it is not defined. Anonymisation may be used by data controllers or data processors to minimise their use or retention of data in an identifiable form where it is not necessary to do so. This is in line with the principles of proportionality, necessity, retention and the storage of personal data. The data controller or data processor must ensure that there is "*no possibility* of re-identification of anonymous personal data" and that this is properly tested. The inclusion of the phrase 'no possibility' and the requirement for this to be tested suggests that for data to be considered anonymised, the anonymisation must be proved through testing to be effective and absolute. Again, the PDPA does not mention 'pseudonymised data', but the term is used in the Regulations, although it is not defined. It is, however, clearly used as a safety measure that involves "storing identification keys separately".

GDPR guidance on how to make an assessment to determine whether data is anonymous

Without clear guidance on what constitutes anonymised data, 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 anonymisation techniques. There is some uncertainty, however, which relates to the perspective from whom we consider whether the data is anonymised.

On this there are two possibilities:

(1) Is there anyone in the world who can identify the data subject from the data? (objective test)
(2) Can a specific holder of the data identify the data subject from the data? (objective test, which is context-specific, and so is considered from the data recipient's point of view.)

The first possibility 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 Data 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 Data 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.

Without direction from the Commissioner on a test, it will be for the data controller to decide.

Guidance related to anonymisation under the GDPR

In making this decision, there are general points that may be worth keeping 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 on the current state of the art. As technology progresses, data that was once deemed to be anonymous may become personal data and thus 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.
- Possibly follow the GDPR test that 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 considered to be sensitive personal data. It not only falls under the data protection law but also 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 – i.e., the objective factors related to the data.

Key Principles That Must be Met in the Personal Data Protection Act

1. *Lawfulness, fairness, and transparency*: 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. The processing of sensitive personal data is generally not permitted unless it falls within one of the grounds in the PDPA. There is a special provision on the processing of sensitive personal data. The provision states that written consent of the data subject prior to processing sensitive data is not required where the processing is necessary for scientific research and the Commission has, by special guidelines, specified the circumstances under which such processing may be undertaken.
2. Personal data is collected for explicit, specified and legitimate purposes and is not further processed in a manner incompatible with those purposes (purpose limitation).
3. Personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (data minimisation).

4. *Accuracy*: Personal data must be accurate and, where necessary, kept up to date, with every reasonable step taken to ensure that any inaccurate personal data is erased or rectified without delay.
5. *Storage limitation*: Personal data should be kept in a form that 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.
6. *Data subject rights*: Personal data should be processed in accordance with the rights of the data subject.
7. *Security*: Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against any loss, destruction or damage, using appropriate technical or organisational measures.
8. *Cross-border transfer of data*: Personal data should not be transferred abroad contrary to the provisions of the law.

Data Subject Rights Under the Personal Data Protection Act

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

(1) *Right to be informed*: The data subject has the right be informed that his/her data is being processed and about the purposes of that processing. The data subject is also entitled to be informed by the data controller of the logic involved in decision-making where the automatic processing of personal data for evaluating matters relating to a data subject has constituted or is likely to constitute the sole basis for any decision significantly affecting the data subject.

(2) *Right to prevent processing*: The data subject has the right to prevent or to suspend the processing of his/her personal data by a data controller if the processing is likely to cause substantial damage to him/her or to another person.

(3) *Right to prevent processing of personal data for direct marketing purposes*: The data subject may require the data controller to stop processing his/her personal data for direct marketing or the processing of personal data for financial benefits.

(4) *Rights in relation to automated decision-making and profiling*: The data subject has the right to object to a decision based solely on automated processing unless it falls in one of the three categories exempted in law, including a data subject's explicit consent. The procedure for notification of a data subject where a decision which significantly affects the data subject is based solely on the processing by automatic means, is in the Regulations.

(5) *Right to compensation*: The data subject has a right to compensation if he/she suffers damage by reason of any contravention of any of the requirements of the PDPA.

(6) *Right to rectification, blocking, erasure and destruction of personal data*: The data subject, on application to the Commission, may cause it to order the data controller or data processor to rectify, block, erase, or destroy personal data. The procedure to be followed for erasure is set out in section 17 of the Regulations.

Cross-Border Data Sharing

Each of the provisions applies to research that uses personal data. Personal data protection law also has additional provisions that must be met when personal data is 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.

Transborder (cross-border) data flow is defined as "any international cross-border flows of personal data by means of electronic transmission or other means". It *could* also include where a researcher outside of the country accesses 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 applies or not in these contexts is not settled law.

Legal bases for transferring personal data outside of Tanzania

In addition, there must be a ground under which the transfer can occur. In terms of the PDPA, the *legal bases* for transferring personal data out of Tanzania are:

1. *Adequacy*: A transfer of personal data to another country can occur where the country has a legal framework that provides for adequate data protection if:

   (a) the recipient establishes that the personal data is necessary for the performance of a task carried out in the public interest or for a purpose related to the lawful functions of a data controller; or

   (b) the recipient establishes the necessity of having the data transferred and there is no reason to assume that the data subject's legitimate interests may be prejudiced by the transfer or the processing in the recipient country.

   The data controller must make an initial assessment of the necessity of the transfer and the recipient of the data must verify the necessity of the transfer. The data controller must ensure that the recipient processes the personal data for the purposes for which it was transferred.

2. If a country does not have a relevant legal framework that provides for an adequate level of protection, cross-border transfer of data can also take place if an adequate level of protection is ensured in the country of the recipient and if the personal data is transferred solely to permit processing authorised to be undertaken by the data controller. An assessment of adequacy is made taking into consideration: all the circumstances of the relevant personal data transfer; the nature of the personal data; the purpose and duration of the proposed processing; the recipient country; the relevant laws in force in the third country; and the professional rules and security measures that are complied with in the recipient country.

A transfer can take place to a country that does not have an adequate level of protection on the following grounds:

1. The data subject has consented to the proposed transfer;
2. Transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of precontractual measures taken in response to the data subject's request;

3. The transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the data controller and a third party in the interest of the data subject;
4. The transfer is necessary or legally required on public interest grounds, or for the institution, trial or defence of legal claims;
5. The transfer is necessary in order to protect the legitimate interests of the data subject;
6. The transfer is made in accordance with the law, and is intended to provide information to the public, and is open for consultation either by the public or by any person who can demonstrate a legitimate interest to give his/her opinion in accordance with the conditions provided under the law; and
7. The Commission may authorise a transfer of personal data to a recipient country or any other country which does not have an adequate level of protection in its laws if the data controller satisfies the Commission that there are adequate safeguards for the protection of personal data, the fundamental rights and freedoms of the data subject and the exercise of the data subject's rights, and that such safeguards can be appropriated through adequate legal and security measures and contractual clauses.

Procedure for transferring personal data outside of Tanzania (including information required by the application)

The procedure for transferring personal data outside of Tanzania is set out in the Regulations. A data controller or data processor who intends to transfer personal data outside of the country must apply for a permit using Form No. 7 which is set out in the First Schedule to these Regulations. The application must include the following information:

- particulars of the applicant, recipient and data subject;
- the type of personal data to be transferred;
- the purpose and necessity of transferring personal data;
- details of the security of personal data in the country of the recipient;
- consent of the data subject;
- date and time of sending personal data; and
- any other information required by the Commission.

In addition, at the time of application, proof must be submitted that

- the country receiving the personal data has ratified an international agreement providing requirements for the protection of personal data;
- there is an agreement between the Tanzania and the country receiving the personal data on the protection of personal data; or
- there is a contractual agreement between the person requesting the personal data and the recipient of the personal data who is outside of the country.

Reasons for rejection of an application

The Commission must consider an application within 14 days, after which time it can reject or approve a permit. An application may be rejected for the following reasons:

- the transfer of personal data endangers national security;
- the Commission is satisfied that there is no adequate protection of personal data in the country of the recipient;
- the transfer of personal data is restricted by other written laws;
- application for a permit to transfer personal data does not meet the requirements of Regulation 20;
- other reasonable grounds which the Commission may deem necessary in the public interest.

The permit will be issued subject to the following conditions:

- The personal data must be transferred to the recipient authorised in the permit.
- The personal data transferred must be processed for the intended purpose only.
- The personal data must not be disclosed or transferred to another recipient without the approval of the Commission.
- The processing of personal data outside of the country must not violate the laws of the country.

Legal Regulation of AI

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

There is no specific AI legislation in Tanzania and there are no particular legislative provisions that address AI-related issues, including predictive algorithms. Furthermore, there is no technological provision or industry/sector-specific guidance for AI. Therefore, it is necessary to consider the legal landscape in relation to 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

Tanzania does not have a specific AI strategy but policy documents speak to the importance of AI for innovation. These documents mention AI and how digital solutions can help improve various sectors in Tanzania.

National Information and Communications Technology Policy, 2016

This provides a framework to help develop the Tanzanian economy by the use of ICT. Policy objectives include:

- strengthening strategic ICT leadership;
- enhancing access and availability of broadband;
- developing interoperable and sustainable ICT infrastructure that supports national connectivity;
- providing universal access to ICT products and services.

Tanzania Commission for Science and Technology Communication Strategy 2021/22–2023/24 (COSTECH)

COSTECH provides services to relevant stakeholders and these are set out in the Strategy. These include:

- the registration of technologies from abroad;
- reports on these found in accessible databases;
- information on approved technologies provided to the public and private sectors and NGOs.

Much of the monitoring and evaluation of the effectiveness of the implementation of this Strategy depends on feedback given by the relevant stakeholders.

The National Health Policy, 2017

The Policy defines health technologies and medical devices. As a policy statement, the government will strengthen the national support systems for assistive devices, other medical supplies, and equipment.

Health Sector Strategic Plan July 2021 to June 2026

This aims to strengthen ICT usage for improved health and support services. Increased access to quality diagnostic services is understood to be realised through the use of emerging technologies, as patients in understaffed facilities may be assisted via telemedicine. With ICT, government is developing sustainable ICT systems in data management, processing and reporting, medical decision-making, and e-learning for health workers. It has defined regulations for interoperability and harmonisation of systems. The government has developed a national investment plan to guide all partners in ICT development and will establish a Centre for Digital Health. Government will establish a legal framework for protecting the security of data, privacy, and the confidentiality of patients. There will be regulations for the use of personal data for management and research.

Specific objectives of the plan include:

- increased access to services using emerging technologies;
- using a national and international referral system;
- increased efficiency in providing and monitoring healthcare using ICT.

Digital Health Strategy, 2019-2024

Strategic priorities of this Strategy include**:**

1. strengthening digital health governance and leadership to facilitate better coordination and implementation of digital health initiatives;
2. improving efficiency, accessibility (including use of telehealth), patient safety, and quality and continuity of care through holistic digitalisation of health service delivery;
3. improving health workforce competency and use of technology to provide specialised care to under-served facilities;
4. promoting healthy behaviour through access to relevant health information, education, and communication;
5. enhancing seamless and secure information exchange;
6. improving data use for evidence-based actions at all levels of the health system;
7. improving supply chain management of health commodities at all levels of the health system;
8. improving management of human resources at all levels of the health system;
9. improving management of financial resources;
10. strengthening disease prevention, surveillance, detection, reporting, response, and control at all levels of the health system.

The Strategy outlines the issues faced in the medical sector and potential solutions to curb these problems by using digital health responses. It recognises that the use of artificial intelligence (big data analytics and machine learning) can help increase the effectiveness of health service delivery and promote UHC.

Tanzania Digital Health Investment Roadmap, 2017–2023

This report describes the 17 investment recommendations prioritised by the Government of Tanzania to improve health system performance through better data use. The recommendations

for investment help: enhanced service delivery, health system performance, resource management, data supply and demand, and the connection and harmonisation of data systems. The report highlights the need for a National eHealth Standards Framework as Tanzania possesses the digital health infrastructure and governance to ensure standards-based and interoperable data systems, irrespective of the technologies on which they are based. In the country there is consensus on 'content, coding, and communication formats, enabling more effective data sharing and use'.

Some investments were not included as part of the planned costs in this plan:

- developing an eLearning platform for health workers and provider communications;
- establishing provider-to-provider telemedicine processes;
- enabling two-way health information communications and provider–client telemedicine.

Digital Health/E-Health

The Digital Health Strategy 2019–2024 and Tanzania's Digital Health Investment Road Map 2017–2023 guide digital health initiatives. The Medical Council of Tanganyika (Exams and Registration Procedures) Regulations, 2018 and the Code of Ethics and Professional Conduct for Medical and Dental Practitioners in Tanzania, 2005 regulate the medical conduct of healthcare practitioners. Medical research is regulated by the National Institute for Medical Research Act. The Tanzania Medicines and Medical Devices Act regulates medical devices and is enforced by the Tanzania Medicines and Medical Devices Authority.

Additional regulations guiding medical devices include The Tanzania Medicines and Medical Devices (Control of Medical Devices) Regulations and the Tanzania Medicines and Medical Devices (List of Registered Human Medicinal Product Veterinary Pharmaceutical and Medical Devices).

No specific legislation governs AI use in healthcare.

Consumer Protection & ICT/E-Legislation

Consumer Protection	Fair Competition Act
ICT/E-Legislation	Cyber Crimes Act Electronic and Postal Communications (Computer Emergency Response Team) Regulations Electronic and Postal Communications (Consumer Protection) Regulations Electronic and Postal Communications (Electronic Communication Numbering and Addressing) Regulations Electronic and Postal Communications (Interconnection) Regulations Electronic and Postal Communications (Investigation) Regulations Electronic and Postal Communications (Licensing) Regulations Electronic and Postal Communications (Online Content) Regulations Electronic and Postal Communications (Quality of Service) Regulations Electronic and Postal Communications (Tariffs) Regulations Electronic and Postal Communications Act Electronic Transactions Act Tanzania Communications Regulatory Authority Act

Data Protection

No single law with comprehensive provisions governs data protection.

Personal Data Protection Act

The PDPA intends to entrench individual rights to personal identity and privacy and, further, will also set appropriate procedures for collecting, storing, processing and disseminating personal information. There are also various statutes and regulations containing data protection provisions relevant to the industry or sector.

Relevant legislation

Provisions on data protection can be found in various pieces of legislation, such as the Constitution. Furthermore, the Electronic and Postal Communications Act (EPOCA) governs electronic, telecommunications and postal communications in Tanzania and is enforced by the Tanzania Communications and Regulatory Authority (TCRA). In addition, the Cybercrimes Act provides for offences related to violations of privacy in respect of using a computer system located in

Tanzania. There are also notable requirements in the financial sector through the Bank of Tanzania (Credit Reference Bureau) Regulations.

Date Use Partnership

The Ministry of Communication and Information Technology seeks to improve the technological landscape and the government is running the Data Use Partnership which has a well defined data management aspect. The Data Use Partnership is a Tanzanian government-led initiative that is improving the national healthcare system through better digital health systems and the use of health information.

Intellectual Property

Tanzania is a member of the African Regional Intellectual Property Organization (ARIPO) and the World Intellectual Property Organization (WIPO). The Constitution allows ownership of intellectual property and guarantees its protection. Accordingly, laws have been enacted to promote and protect intellectual property rights. The Copyright Society of Tanzania (CST) administers the registration of copyrights. The registration of trademarks and patents is administered by the Business Registration and Licensing Agency.

Relevant Acts and Regulations are:

The Patents (Registration) Act (Patents Act)

The Patents Act defines patentability by using the word "invention". This means there is "a solution to a specific problem in the field of technology and may relate to a product or process". Furthermore, an invention is patentable if it is new, involves an inventive step, and is industrially applicable.

Fair Competition Act

The definition of "business records" in this Act covers:

(a) accounts, balance sheets, vouchers, records, minutes of meetings, contracts, files, instructions to employees and other persons, and includes a person carrying on business as a broker.

(b) any information recorded or stored by a computer or other device and any material subsequently derived from information so recorded or stored.

Copyright and Neighbouring Rights Act (Copyright Act)

The Act defines computer and computer program:

> "Computer"' means an electronic or similar device having information processing capabilities. "Computer Program" means a set of instructions expressed in words, codes, schemes or in any other form, which is capable when incorporated in a medium that the computer can read, of causing a computer to perform or achieve a particular task or result.

The Copyright Act explains what will be considered as works in which copyright may subsist and protection will be afforded. However, "mere data" will not be protected.

Copyright Licensing and Rights to Benefit from Re-Sale Regulations

- The Regulations prohibit public performance, communication, reproduction, or broadcasting of a work that is copyright protected. This can only be done if a licence is granted by the Copyright Society of Tanzania. Permission is required from the owner if the work is protected and it is used in accordance with the Copyright Act.
- Contracts entered into regarding copyrights in Tanzania must be given to the CST before they are operational.
- The CST receives licence applications and application fees must be paid according to the Third Schedule to the Regulations. Thereafter, the CST issues a licence valid for the purpose it has been issued and for a specific period.

Summary and Analysis

While several ICT policy documents that support 4IR enablement have been produced, relevant provisions in legislation take precedence over other regulatory/policy documents. Focus areas include strengthening of ICT infrastructure and increased accessibility to information on new and emerging technologies. Policy documents that encourage the use of ICT and emerging technologies to improve health service delivery through telemedicine and evidence-based

decision-making are important. While policy documents guide digital health implementation, there is no specific legislation governing AI use in healthcare. The policy documents are interoperable and do not supersede one another.

Tanzania has data protection legislation in the form of the Personal Data Protection Act. However, provisions on data protection can be found in various other pieces of legislation, such as the Electronic and Postal Communications Act and the Cybercrimes Act. AI technologies may receive some protection under the Fair Competition Act.

ICT/E-legislation and a consideration of IP legislation, jurisprudence and soft law may be essential for ensuring that the technologies are used properly.