ZIMBABWE

ACRONYMS

4IR	Fourth Industrial Revolution
AI	Artificial intelligence
ARIPO	African Regional Intellectual Property Organization
DPA	Data Protection Act
EU	European Union
GDPR	General Data Protection Regulation (Europe)
GIS	Geographical information system
HBM	Human biological material
HPC	High performance computing
ICT	Information and communication technology
IP	Intellectual property
IT	Information technology
MCAZ	Medicines Control Agency of Zimbabwe
NHRDC	National Health Research Development Committee
NIE	National internet exchange
PI	Principal investigator
POTRAZ	Postal and Telecommunications Regulatory Authority
RCZ	Research Council of Zimbabwe
SADC	Southern African Development Community
STI	Science, Technology and Innovation
ZINGSA	Zimbabwean National Geospatial and Space Agency
WIPO	World Intellectual Property Organization
ZCHPC	Zimbabwe Centre for High Performance Computing

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 main data protection legislation is the Data Protection Act (DPA) (2021). The standard is specific informed consent.

Data Protection Act

Genetic data and DNA (analysis)

Genetic data is defined as referring to any personal information stemming from a DNA analysis. Therefore, the information as opposed to the DNA itself is contemplated as genetic data, and such information about an individual is also classified as sensitive data.

Consent and processing of sensitive data/genetic data

The processing of sensitive data, including genetic data, may only be undertaken with the consent of the data subject or of a competent person where the data subject is a child. Consent is not required to process non-sensitive data. Genetic data is treated as sensitive data and therefore consent will apply and must be in writing to allow processing. The data subject can withdraw consent at any time without any explanation and this is free of charge.

Exemptions from consent

Consent of the data subject is exempted for scientific research, subject to the conditions set by the data protection authority. Consent may also not be required when the processing is necessary for preventive medicine or medical diagnosis; the provision of care or treatment for the data subject or to one of his or her relatives; the management of healthcare services in the interest of the data subject; and when the data is processed under the supervision of a health professional.

Prohibition of processing of certain sensitive data by data protection authority

The data protection authority can prohibit the processing of certain sensitive data even when the data subject has consented – considering the factors associated with the prohibition and the reasons for collecting the data.

Transfer of personal data to another country which does not offer adequate protection may be possible

Adequate levels of protection are required with the transfer of personal information about a data subject to a third party in a foreign country. However, it is still possible to transfer data to a country outside Zimbabwe which does not assure an adequate level of protection in certain circumstances – including where the data subject has unambiguously given his or her consent to the proposed transfer.

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. These include the right to freedom of expression, including artistic expression and scientific research and creativity, and the right to inherent dignity. These rights are pronounced in the Constitution but are implemented in laws, regulations and guidelines.

Regulatory and Supporting Institutions

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

- Medical Research Council of Zimbabwe
- Medicines Control Authority of Zimbabwe
- Ministry of Health and Childcare
- National Biotechnology Authority of Zimbabwe
- National Blood Service Zimbabwe
- Research Council of Zimbabwe.

Individual and Community Benefit Sharing

The approach to benefit sharing is as follows. With respect to research on human participants, the investigators are required to do a proper risk and benefit analysis of the study and inform the research participants of the benefits and harms beyond the duration of the research. The law is not elaborate on individual and community benefit sharing, but the law and regulations are clear on ensuring that the benefits of the research accrue to the research participants.

Benefits

(1) Tissue donation, removal and associated payment

For any tissue, organ, blood or gametes to be removed from any person, that person must give written consent. The informed consent must be obtained before the start of the research. This requirement is only waived in extenuating circumstances such as a situation of coma, emergency or mental incapacity.

It is a criminal offence to trade human blood, cells, tissues and organs. The only form of payment that can be made is for compensation on account of expenses incurred in the process of donation. This is because matters concerning compensation extend beyond HBM to associated data. Therefore, a person is not entitled to remuneration in relation to a donation of their human biological data. Purpose is limited to health, scientific, research or therapeutic purposes.

(2) Patenting

Patenting is allowed and encouraged. However, a number of inventions cannot be patented. These include: diagnostic, therapeutic or surgical methods for the treatment of human beings or animals; plants and animals, other than micro-organisms, and biological processes for the production of plants or animals. 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

Data Protection Act

The DPA defines personal information as information relating to a data subject, and includes:

(a) the person's name, physical address (geospatial data) or telephone number;
(b) the person's race, national or ethnic origin, colour, religious or political beliefs or associations;
(c) the person's age, sex, sexual orientation, marital status or family status;
(d) an identifying number, symbol or other particulars assigned to that person;
(e) fingerprints, blood type or inheritable characteristics;
(f) information about a person's healthcare history, including a physical or mental disability;
(g) information about educational, financial, criminal or employment history;
(h) opinions expressed about an identifiable person;
(i) the individual's personal views or opinions, except if they are about someone else; and
(j) personal correspondence pertaining to home and family life.

Sensitive personal information/data

Although the DPA further distinguishes between personal information and sensitive personal information, it is doubtful that geospatial information could be considered to be sensitive personal

information because it is not listed, defined or referred to in the definition of sensitive personal information. Sensitive information includes:

- racial or ethnic origin; political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sex life;
- criminal, educational, financial or employment history;
- gender, age, marital status or family status.

These considerations merit special attention by health researchers combining geospatial data with health data in such a way that individuals may be identifiable. The DPA refers to sensitive data as specifically including health information about an individual; genetic information about an individual; or any information which may be considered as presenting a major risk to the rights of the data subject. Therefore, health data and genetic data are specifically mentioned as part of sensitive data under (b) of that definition. The DPA goes further to recognise genetic information. It defines genetic data as any personal information stemming from a DNA analysis.

The DPA refers to sensitive data only. Therefore, sensitive data can be treated differently to personal information, for example. Sensitive data can be processed only if a data subject gives written consent. There are circumstances where the Authority might not allow processing even with consent. There are times where sensitive data can still be processed without consent. Some of these include activities involving non-profit organisations, those in the public interest, to abide by law, and for scientific research purposes (the Authority can make conditions on this).

Processing of health and genetic information

There is a specific rule regarding processing of health and genetic information. The processing of genetic data, biometric data and health data is prohibited unless the data subject has given written

consent to the processing. If written consent is not given, only a healthcare professional can process health data – unless there is an emergency. With regard to genetic data, the processing of genetic data is authorised if it is processed for what it reveals or contains and data concerning health is processed only if a unique patient identifier is given to the patient which is distinct from any other identification number issued by the public Authority established for this purpose. Furthermore, if there is identification, the Authority must give permission.

The Postal and Telecommunications Regulatory Authority

The Postal and Telecommunications Regulatory Authority is designated as the data protection authority. The Authority has a Data Protection Division. In terms of the DPA, one of its functions is, in consultation with the Minister, to facilitate cross-border cooperation in the enforcement of privacy laws and participating at national, regional and international forums mandated to deal with the protection of personal information initiatives.

Research Act

The Act aims to regulate and facilitate research activities in Zimbabwe, ensuring that research is conducted in an ethical and responsible manner and that the results of research contribute positively to the development of the country.

Key provisions:

- *Research Council of Zimbabwe (RCZ)*: The RCZ is established as the regulatory authority responsible for overseeing research activities in the country. It is tasked with promoting and coordinating research efforts.
- *Research permits*: Individuals or organisations intending to conduct research in Zimbabwe may be required to obtain research permits from the RCZ. These permits specify the scope, objectives, and ethical considerations of the research project.
- *Ethical standards*: The Act emphasises the importance of adhering to ethical standards in research. Researchers are expected to conduct their work with integrity and in a manner that respects human rights and the dignity of research subjects.

- *Protection of research data*: The Act addresses the confidentiality and protection of research data. Researchers must take measures to safeguard the privacy and confidentiality of research participants and data.
- *Research reports*: Researchers are expected to submit research reports to the RCZ on completion of their projects. These reports are intended to contribute to the knowledge base of the country and may inform policy and decision-making.
- *Promotion of research*: The Act encourages and supports research efforts that contribute to national development, including research related to agriculture, health, education, technology, and other areas of societal importance.
- *Research funding*: The Act may address mechanisms for funding research, potentially through government grants or other funding sources.
- *Penalties for non-compliance*: The Act may specify penalties for individuals or organisations that fail to comply with its provisions or which conduct research without the required permits.

Role of the Zimbabwean National Geospatial and Space Agency (ZINGSA)

ZINGSA was established by the Research Act to implement any geospatial space programme in line with the policy determined in terms of the Act. ZINGSA will implement a geospatial space programme in line with the policy determined in terms of the Research Act. It will:

- operationalise its administrative framework;
- implement research on fertiliser requirements for different soil types;
- revise agro-ecological zones;
- develop a geological minerals map focusing on lithium and graphite;
- produce a solar potential map for Zimbabwe;
- develop a malaria prevalence map for Zimbabwe;
- develop a bilharzia prevalence map for Zimbabwe;
- develop geodatabases for farms.

ZINGSA is divided into institutes, including Geospatial and Earth Observation. In this programme ZINGSA will conduct specialised research and development on projects and activities on

geospatial applications and Earth observation, including mining and mineral exploration, disaster management, weather, climate, geospatial intelligence, agriculture and ecosystems, water, energy, health, and any other national strategic applications. This programme is responsible for the development and promotion of Earth observation products for socio-economic development and to improve livelihoods in Zimbabwe. It will also develop and maintain a long-term archive of satellite data for national benefit that is essential for change detection for better understanding of heritage and environmental change in time and space. Objectives are:

- remote sensing;
- geospatial data analysis, management, and integration;
- cutting edge GIS research, consultancy, and training;
- development of GIS, and modelling.

Interception of Communications Act

This Act is the primary legislation that governs communications surveillance, but fails to abide by international human rights standards such as the requirement that a competent judicial authority make determinations about communications surveillance.

It provides that all interceptions are implemented such that neither the interception target nor any other unauthorised person is aware of any changes made to fulfil the warrant. The Act severely encroaches on communication rights and freedoms through unregulated surveillance, and therefore potentially undermines the implementation of a just and fair internet governance regime (MISA Zimbabwe 'Internet Governance in Zimbabwe').

The Act criminalises illegal interception, which is defined as interception of communication without consent or authorisation by a warrant. It restricts disclosure of interception information to unauthorised parties, which is punishable with a fine not exceeding Zimbabwe Dollars 1 600 000, imprisonment for up to five years, or both. However, it also provides a legal basis for state authorities to conduct communications surveillance without safeguards, such as the prior authorisation of an independent and impartial judicial authority; due process; and specific

limitation on time, notification of the surveillance and effective monitoring and regular review by an independent oversight mechanism, which are stipulated by the Declaration.

The Act states that individuals aggrieved by the warrant of interception issued by the Postal and Telecommunications Authority may appeal to the Administrative Court, which can make the final decision.

Regulations, Guidelines and Policies

General Notice 483 of 2019 (GN 2019-0483): Establishment of Zimbabwe National Geospatial & Space Agency

The Minister for Higher and Tertiary Education, Science and Technology Development established the Zimbabwe National Geospatial and Space Agency for purposes of research.

The Postal and Telecommunications Regulatory Authority (POTRAZ) requires all telecommunications companies to create a centralised subscriber database of all their users. These regulations require telecommunications companies to implement a system to obtain, record and store, where the customer is a natural person, their full name and permanent residential address – which directly refers to geospatial data. Geospatial data in this context forms part of personal information and deserves the same protections offered in the Data Protection Act. The regulations also require storage of subscriber nationality; gender; subscriber identity number; national identification number; or passport number. Where the customer is a legal person, telecom companies are to record or store:

- a copy of the certificate of registration or incorporation or business licence;
- the full names, surname, national identification number and address of the authorised representative of the legal person;
- the name and address of the juristic person and, where applicable, the registration number of the legal person;
- the subscriber identity number.

Draft e-Health Strategy 2012–2017

The Ministry of Health and Child Welfare notes in relation to e-Health and mobile health solutions that electronic surveillance systems can provide decision-makers with the power to decide on the most appropriate interventions, and a service relevant to the target population.

Key health-related applications that can be used in mobile health include national disease surveillance and monitoring tools. Disease Surveillance and Population-Based Information Systems are a priority area of implementation. In these applications, geospatial data will be a core component of the surveillance mechanisms. A Location Registry will contain a register of all key service locations and associated geographic information system coordinates will be incorporated. Geospatial data in this context is part of personal information and deserves the same protections offered in the Data Protection Act, read with relevant health statutes.

National Policy for Information Communications Technology

This policy objective provides for inclusiveness, bridges the digital divide and provides broadband for all. The objective is to attain universal access to ICT services in the country, which translates to a 100% internet penetration, 80% internet geographical coverage, and affordable services relative to the country's economy and SADC benchmarks. Universal access will drive the domestic market for ICT products and services. In addition, it is a foundation for national innovation and entrepreneurship (Ministry of Information Communication Technology, Postal and Courier Services 'National Policy for Information Communications Technology, 2016'). Geospatial data is not specifically addressed in this context but ICT penetration is an essential stepping stone to developing GIS-driven national spatial health information infrastructure and health surveillance services.

Conclusion and Recommendations

Zimbabwe has begun the process of regulating the use of spatial information, including applications in the field of health. Zimbabwe's Data Protection Act applies to geospatial data that identifies an individual. However, there is a lack of infrastructure to support and develop

integration of any geospatial data and a lack of properly integrated laws to allow for the optimal use and protection of geospatial data in the context of public health emergencies.

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 DPA, 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 DPA and to begin to assist users in navigating the Act. It is not comprehensive, and users of the DPA must consult it to understand all relevant and applicable requirements to be met, and to understand any exceptions that may be in place for research. This is necessary as all these requirements must be met in the processing of personal data for research, in addition to the requirements on cross-border sharing of data.

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

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

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

processes vast quantities of personal information, the Act applies. It is only one of several laws that must be met when transferring data for research.

Health Research Regulations and Cross-Border Data Sharing

In addition to the national laws listed below, several international treaties and conventions have been signed. Of importance in this domain is the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention). However, Zimbabwe has not ratified the Malabo Convention.

The relevant national legislation is:

- Constitution of Zimbabwe
- Research (Constitution of the National Public Health Institute) Regulations, 2020
- Research Act

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

Data Protection Act

In addition to these legal and ethical requirements, the Data Protection Act applies to the processing of all personal information. In an acknowledgment of the importance of research, special provisions are in place for research. Importantly for health research, the processing of genetic data, biometric data, and health data is prohibited unless the data subject has given consent to the processing in writing.

The conditions set out in the Data Protection Act must all be met for research. In addition, there are extra conditions that must be met prior to the transfer of personal information across borders.

Some of the techno-legal terms used in the Data Protection Act are discussed below. This is not a thorough assessment of the Act 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 information for research.

The Main Actors Defined in the Data Protection Act

	Legal definition	**Layman explanation**
Data subject	An individual who is an identifiable person and the subject of data.	The person to whom the data relates.
Data controller	Any natural person or legal person who is licensable by the Authority; this includes public bodies and any other person who determines the purpose and means of processing data.	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 or legal person who processes data for and on behalf of the data controller and under the data controller's instruction, except for the persons who, under the direct employment or similar authority of the data controller, are authorised to process the data.	Someone who is not directly employed by the data controller, but who is processing personal information under the direction of the data controller. They may be a consultant, for example.
Data Protection Authority or Authority	Postal and Telecommunications Regulatory Authority of Zimbabwe, established in terms of the Postal and Telecommunications Act.	The independent body established to monitor and enforce compliance with the DPA.
Data Protection Officer or DPO	Any individual appointed by the data controller and who is charged with ensuring, independently, compliance with the obligations provided for in the DPA.	An individual in an organisation who is appointed to advise and promote compliance with the law.
Data controller's representative or Controller's representative	Any natural person or legal person who performs the functions of the data controller in compliance with obligations set out in the DPA.	

Child	Any person under the age of eighteen years.	
Third party	Any natural or legal person or organisation other than the data subject, the data controller, the data processor and anyone who, under the direct authority of the data controller or data processor, is authorised to process the data.	
Identifiable person	A person who can be identified directly or indirectly, particularly by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.	
Minister	The Minister responsible for information and communications technologies.	
Health professional	Any individual determined as such in terms of the Health Professions Act.	
Recipient	A natural or legal person, agency or any other body to whom personal information is disclosed by a data controller, whether a third party or not. However, persons who receive personal information in the framework of a particular legal inquiry must not be regarded as recipients.	

Categories of Data Listed in the Data Protection Act

	Legal definition	**Layman explanation**
Personal information	Information relating to a data subject, including (a) the person's name, address or telephone number; (b) the person's race, national or ethnic origin, colour, religious or political	Information about a particular person that can identify him or her.

	beliefs or associations; (c) the person's age, sex, sexual orientation, marital status or family status; (d) an identifying number, symbol or other particulars assigned to that person; (e) fingerprints, blood type or inheritable characteristics; (f) information about a person's healthcare history, including a physical or mental disability; (g) information about educational, financial, criminal or employment history; (h) opinions expressed about an identifiable person; (i) the individual's personal views or opinions, except if they are about someone else; and (j) personal correspondence pertaining to home and family life.	
Sensitive data	Information or any opinion about an individual which reveals or contains the following: (a) racial or ethnic origin; (b) political opinions; (c) membership of a political association; (d) religious beliefs or affiliations; (e) philosophical beliefs; (f) membership of a professional or trade association; (g) membership of a trade union; (h) information on sex life; (i) criminal, educational, financial or employment history; (j) gender, age, marital status or family status; (k) health information about an individual; (l) genetic information about an individual; or (m) any information which may be considered as presenting a major risk to the rights of the data subject.	Data about a particular person which is considered sensitive, such as health data and genetic data, and which receives additional legal protection.
Data	Any representation of facts, concepts and information, whether in text, audio, video, images, machine-readable code or instructions, in a form suitable for communications, interpretation or processing in a computer device/system, database, electronic communications network or	

	related devices and including a computer program and traffic data.	
Genetic data	Any personal information deriving from a DNA analysis.	

Generally, data protection law applies only to personal data. The Data Protection Act, however, applies to the processing of all data as defined in the Act. Despite this, many of the restrictive provisions concerning the processing and transfer of data relate specifically to personal information (and not to data generally). Therefore, if data is not considered to be personal data, a researcher may be exempt from the more restrictive processing requirements.

Different sections of the DPA refer to "personal information" and "data". This does not imply that the terms can be used interchangeably as "personal information" is best described as information which can be used to identify a data subject, clearly indicating that it is specific to the data subject and his/her unique features (e.g., racial origin, gender, genetic information). In contrast, "data" has a broader meaning as it simply includes whatever representation of facts or information can be conveyed on a digital platform, such as a computer system, computer device or a database.

Researchers, however, must still be careful when considering the transfer of data outside of Zimbabwe. The Act sets out the requirements for the transfer of *personal information* outside of Zimbabwe and the requirements for the transfer of *data* outside of Zimbabwe. Before considering the requirements, a researcher must know when the Act applies.

Many other data protection regulations state that anonymised or de-identified information that cannot be re-identified is not considered to be personal data and therefore does not fall under the Act concerned. Zimbabwe, however, does not do that. Pseudonymisation is also not specifically mentioned. The DPA does provide that "data concerning health shall be processed only if a unique patient identifier is given to the patient which is distinct from any other identification number issued by the public authority established for this purpose". This is often what is defined as pseudonymisation and is a technique that is a requirement for the lawful processing of health data. The linking of the patient identifier to another identifier that allows the data subject to be

identified is permissible only with the Authority's express permission. This, however, does not appear to exempt the data from the application of the DPA. More clarity from the Authority is needed on whether the pseudonymised dataset would be considered personal information in the hands of a recipient who does not possess the means to re-identify the data subject.

Researchers will need to make an assessment about whether the data they are holding is personal data. This is difficult in the absence of guidance from the Authority. Researchers *may* want to follow the guidance provided under the EU General Data Protection Regulation 2016/679 (GDPR), which sets out how to make an assessment to determine whether data is anonymous (and therefore the data that falls outside of the GDPR), and outlines several anonymisation techniques. There is some uncertainty in this area, however, which relates to the perspective of the data holder who is considering 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? (This is an objective test that determines whether anyone would be able to identify the data subject.)
(2) Can a specific holder of the data identify the data subject from the data? (This is a context-specific test from the perspective of the data recipient, and whether he or she would be able to identify the data subject.)

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 second 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.

Without direction from the Authority on a test, the data controller will need to decide. In making this decision, general points 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 information and therefore fall under data protection laws.
- 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 considered to be sensitive data. It not only falls under the data protection laws, but also has a higher level of protection.
- There is ongoing debate about whether genomic datasets can ever be rendered truly anonymised, in particular as genetic data is an identifier. The DPA specifically defines genetic data as "any *personal* information" (emphasis added) derived from DNA analysis. In considering whether a genomic dataset can be considered anonymised, context matters – i.e., the objective factors associated with the data.

As mentioned above, special care must be taken to comply with the regulations of the DPA which deal with data generally as these will presumably apply to anonymised data. Anonymised data will be exempt only from provisions specifically concerned with personal information. Until the Authority provides more clarity in this regard, a cautious approach is recommended.

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

1. *Data quality*: The data controller must ensure that personal information is adequate, relevant and not excessive considering its purpose, accurate, and kept up to date (where necessary), and that it is kept in a form that allows for the identification of data subjects for no longer than is necessary.
2. *Accessibility*: The data controller must take appropriate steps to ensure that personal information is accessible regardless of the technology used and ensure that the evolution of technology is not an obstacle to the accessing or processing of such data.
3. *Lawfulness and fairness*: Personal information must be processed lawfully, fairly, transparently, and the processing must be necessary. Lawful means that there must be a legal basis for the processing of the personal information. The processing of sensitive data or genetic data, biometric data, and health data is generally not permitted unless it falls within one of the grounds in the DPA. There is a special provision for the processing of sensitive data or genetic data, biometric data, and health data for scientific research.
4. *Consent and lawful basis*: Non-sensitive personal information may be processed only if the data subject has consented to the processing, unless it is necessary in: (a) proving an offence; (b) complying with an obligation to which the data controller is subject by virtue of a law; (c) protecting the vital interests of the data subject; (d) performing a task carried out in the public interest, or in the exercise of the official authority vested in the data controller, or in a third party to whom the data is disclosed; or (e) promoting the legitimate interests of the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.
5. *Privacy*: Personal information must be processed in accordance with the right to privacy of the data subject. Furthermore, personal information should be collected only where a valid explanation is provided whenever information relating to family or private affairs is required.
6. *Purpose limitation*: Personal information should be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means that the purpose must be clearly set out. The further processing of data for scientific research purposes is not considered incompatible.

7. *Data minimisation*: Only the personal information that is necessary for the specific purpose should be collected and processed. The personal information must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
8. *Accuracy*: Personal information must be accurate and, where necessary, kept up to date.
9. *Storage limitation*: Personal information 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 information is processed. 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.
10. *Disclosure*: When collecting personal information from the data subject (directly or indirectly), the data controller must provide the data subject with certain information, including the details of the data controller, the purpose of the processing, the existence of the right to object, whether compliance with the request for information is compulsory, and any other supporting information. When personal information is not directly obtained from the data subject and is for research purposes, there is no need to comply with the disclosure requirement.
11. *Security*: To protect the security, integrity and confidentiality of the personal information, the data controller must protect the personal information from 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.
12. *Accountability*: The data controller is responsible for, and must be able to demonstrate compliance with, the principles mentioned above. It is good practice to keep a record of data processing activities, measures introduced to protect the data, and any risk assessments made. This can be used to demonstrate compliance in the event of a breach.

Data Subject Rights Under the Data Protection Act

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

1. *Right to privacy*: The data controller must process personal information in accordance with the data subject's right to privacy.
2. *Right to be informed*: The data subject has the right to be informed about what his/her personal information will be used for. This provision can be exempted from if the personal information has not been collected directly from the data subject and the processing is for scientific research purposes and it would be impossible or would involve a disproportionate effort to inform the data subjects.
3. *Right to access*: The data subject has the right to access personal information that the data controller or data processor has about him/her.
4. *Right to object*: The data subject has the right to object to the processing of all or part of his/her personal information, where the lawful basis of processing is not consent.
5. *Right to correction*: The data subject has the right to have false or misleading personal information corrected. The data controller has a duty to erase or rectify any inaccurate personal information.
6. *Right to deletion*: The data subject has the right to have false or misleading personal information about him/her deleted.
7. *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, including profiling.

Cross-Border Data Sharing

When considering the transborder/cross-border flow of personal information for research, all the provisions of the Data Protection Act must be met. The DPA also has a number of provisions on the cross-border flow of personal information that, in addition to the other provisions, must be met.

The DPA defines "transborder flow" as "international flows of data by the means of transmission including data transmission electronically or by satellite".

A data controller is prohibited from transferring personal information about a data subject to a third party in another country. However, there are grounds under which the transfer of *personal information* (but not data) outside of Zimbabwe can take place. They are:

Adequacy: A country or international organisation has an adequate level of protection and the data is transferred solely to allow tasks covered by the competence of the controller to be carried out. The adequacy of the level of protection afforded by the country will be assessed in the light of all the circumstances of a data transfer operation. Particular consideration is given to the nature of the data, the purpose and duration of the proposed processing operation, the recipient country, the laws relating to data protection in force in the country, and the professional rules and security measures which are complied with in that country.

The Authority can lay down the categories of processing operations for which and the circumstances under which the transfer of data to countries outside of Zimbabwe is not authorised. It is important to check that your research does not fall into one of the prohibited grounds.

The Minister responsible for the Cyber security and Monitoring Centre may give directions on how to implement these provisions in terms of the transfer of personal information outside of Zimbabwe. For now, no directions have been provided by the Minister.

For countries without an adequate level of protection, the transfer of personal information and data outside of Zimbabwe can take place only if:

1. The data subject has unambiguously consented to the proposed transfer;
2. The transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of pre-contractual 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 important public interest grounds, or for the establishment, exercise or defence of legal claims;
5. The transfer is necessary in order to protect the vital interests of the data subject;
6. The transfer is made from a register which, according to Acts or Regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the case at hand.

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 Zimbabwe. There is also no particular legislative provision that addresses AI-related issues including predictive algorithms. 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; (4) Data protection law; and (5) Intellectual property.

AI Strategy

There are ongoing initiatives to guide the development of AI at national level. Zimbabwe has launched an AI strategy, developed an AI policy, enacted legislation to address some of the challenges of AI, established a Centre of Excellence on AI, and issued ethical guidelines for AI. A specialised agency in the government has been developed, although a coordinated response cutting across all ministries is yet to be developed. A Cyber and Data Protection Act is part of the AI strategy. AI as a concept has not yet been fully embraced by Zimbabwe, and therefore there is a general neglect with regard to incorporating AI-specific provisions into law.

Policy documents and strategies speak to the importance of AI for innovation and technology. These include:

Zimbabwe National Policy for Information and Communications Technology, 2016

This provides for the establishment of a national data centre using cloud computing opportunities, in a bid to centralise data storage. A National Internet Exchange (NIE) will ensure localised

internet exchange. The strategy further provides for several ICT goals, including transformation, growth, leadership, inclusiveness, sustainability, innovation and partnership.

Science, Technology and Innovation (STI) Policy of Zimbabwe, 2012

Primary goals of the Policy include: strengthening capacity development in STI, learning and using emergent technologies to accelerate development, accelerating commercialisation of research results, searching for scientific solutions to global environmental challenges, mobilising resources and fostering international collaboration in STI. The Policy highlights the need to consider research in the creation of IT platforms for innovative deployment of data and knowledge for use in various sectors of the economy, and to enhance national competence for promoting and supporting computer hardware, software engineering, and cybersecurity.

Zimbabwe Centre for High Performance Computing (ZCHPC) Usage Policy, 2016

The ZCHPC is established in terms of the Manpower Planning and Development Act. The Statutory Instrument 168 establishes and governs ZCHPC operations. The Zimbabwe High Performance Computing Project was conceived in 2011 and HPC was identified as one of the key solutions to help solve challenges associated with climate change, food security, unclean water, poverty, diseases, energy, and human capital development. The HPC Usage Policy is a Sector-Specific Cyber Security Policy meant to safeguard the ZCHPC technical resources from abuse. The Policy provides that exporting software, technical information, encryption software or technology in violation of any international, regional or local export-control laws is prohibited.

Zimbabwe's E-Health Strategy, 2012–2017

The vision of the Strategy is to provide accessible health information on an integrated platform and to ensure: total interoperability among health institutions, timely and limitless access to health information through ICT, seamless running of health functions and services on a single integrated platform, and a seamless electronic health information system available nationwide to facilitate information access and sharing for quality healthcare delivery. The Strategy aims to promote the use of effective health IT in the country while maximising the use of available resources.

Digital Health/E-Health

Zimbabwe's e-Health strategy 2012–2017 guides digital health. It is now part of broader health policy and an e-Health Strategy for 2021–2025 is possible. There is no standalone e-healthcare legislation but provisions that deal with e-Health are embedded in broader healthcare legislation: the Public Health Act. The Health Profession Act regulates healthcare practitioners. The National Health Research Development Committee (NHRDC) provides oversight on all health research conducted in Zimbabwe. Medical research is regulated by the Public Health Act and the Health Research Act. No legislation specifically addresses AI or software as a medical device in Zimbabwe. Medical devices are largely unregulated but the use of such devices, considered administration of medical services, is regulated by the Medicines Control Agency of Zimbabwe (MCAZ).

Data Protection

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 Act. Relevant provisions include rights to opt-in/opt-out, notice and consent requirements and restrictions on offshore data transfers.

Data Protection Act minimum standards for data

Six minimum standards of data collected fairly and lawfully include:

(1) data is to be used only for the specified purpose for which it was originally collected;
(2) data is to be adequate, relevant and not excessive to purpose;
(3) data is to be accurate and up to date;
(4) data is to be accessible to the data subject;
(5) data is to be kept secure;
(6) data is to be destroyed after its purpose is completed.

Restrictions on the processing of sensitive data

Sensitive data can be processed only if a data subject gives written consent. There are circumstances where the Authority may not allow processing – even with consent. There are also times where sensitive data can still be processed without consent, including activities involving non-profit organisations, in the public interest, to abide by law, and for scientific research (the Authority can make conditions on this). Processing of genetic data, biometric sensitive data and health data is not allowed without the necessary written consent of the data subject. Furthermore, this consent can be withdrawn without consequences. If the data subject has not given specific written consent, only a healthcare professional can process health-related data. However, if there is a potential for any danger, the processing does not have to be done by a healthcare professional. A unique patient identifier will be given when processing health data. With genetic data, it will be authorised if it is processed for what it reveals or contains.

Prohibition on automated decision-making

There is a general prohibition on decisions based solely on the automated processing of personal data. The only exceptions to this general prohibition are instances in which the data subject has consented to such a decision or where the processing is based on a provision established by law.

Consumer Protection & ICT/E-Legislation

Consumer Protection	Consumer Protection Act
ICT/E-legislation	Postal and Telecommunications Act (broadly covers ICT and its regulation) Interception of Communications Act Postal and Telecommunications (Telecommunications Traffic Monitoring System) Regulations Postal and Telecommunications (Licensing, Registration and Certification) Regulations Postal and Telecommunications Act International Telecommunications Services Regulations Postal and Telecommunications Internet Services Regulations Criminal Law (Codification and Reform) Act Zimbabwe Media Commission Act

Intellectual Property

Zimbabwe is a member of the African Regional Intellectual Property Organization (ARIPO) and the World Intellectual Property Organization (WIPO). The Copyright and Neighbouring Rights Collecting Society of Zimbabwe, established by the Copyright and Neighbouring Rights Act, is a corporate body that authorises and maintains the registration of copyrighted works.

The Patents Act

The Act does not mention any terms related to computers or technology. The criteria on what would constitute patentability is mentioned only in a schedule which sets out the Protocol on Patents and Industrial Designs within the framework of ARIPO. It provides that the Patents Act should comply with the Protocol.

The Protocol states:

> The Office shall undertake, or arrange for, the substantive examination of the patent application. If it finds that the invention claimed in the application does not comply with the requirements of patentability … it shall refuse the application.

Copyright and Neighbouring Rights Act

The Copyright Act protects real rights in a person's work and extends to a public computer network. It restricts the reproduction or dissemination of copyright material on the internet without the exclusive approval of the copyright owner. Broadcasting on the internet is prohibited.

The Copyright Act sets out definitions of computer programs and literary work. The Act extends to AI technologies and creations in certain instances. It provides that a computer program refers to a set of instructions which is fixed or stored in any manner and which, when used directly or indirectly in a computer, directs its operation to perform a task or bring about a result. Literary work includes:

> Work which is written, spoken or sung, irrespective of its literary quality or the mode or form in which it is expressed, and includes
> (a) dramatic works, stage directions, film scenarios and broadcasting scripts; and

(b) letters, reports and memoranda; and

(e) lectures, speeches and sermons; and

(d) computer programs; and

(e) tables and compilations;

but does not include musical works.

The Copyright Act further sets out what constitutes a public computer network. It states that it means:

> A group of interlinked computers to which the public or a section of the public have access, whether on payment of a fee or otherwise, and includes the computer network commonly known as the Internet.

The Copyright Act also provides:

> Subject to this Act, a work shall be regarded as published
> *(a)* if copies of the work are issued to the public; or
> *(b)* if the work is made available to the public
> (i) by means of an electronic retrieval system; or
> (ii) through a public computer network; or
> (iii) by a public library or archive or other such non-profit-making institution for the purposes of public lending.

The Act also mentions the term 'computer program' in provisions relating to the extent of protection afforded to these works, the ways in which infringement could occur, and the rights afforded to the owner.

Intellectual Property Tribunal Act

The Act establishes the Intellectual Property Tribunal. The Act provides that this Tribunal have the function of dealing with applications and appeals when it comes to matters referred to in the Patents Act and Copyrights Act, among others.

Soft law

The Zimbabwe National Intellectual Property Policy and Implementation Strategy 2018–2022 (the Policy) is the first of its kind in Zimbabwe. As part of the implementation strategy of the Policy, it provides for the establishment of Technology and Innovation Support Centres. These will allow for research sharing and training on patent database access, and will provide access to patent materials that will be important for capacity-building involving technology and innovation.

Summary and Analysis

While Zimbabwe has developed an AI strategy, the necessary instruments are not publicly available. Several ICT policy documents that support 4IR enablement have been produced but relevant provisions in promulgated legislation will take precedence over other regulatory/policy documents. The above policy documents are interoperable and do not supersede one another. Focus areas include strengthening ICT and data infrastructure, increasing research and innovation, and developing a cybersecurity framework. While these instruments do not directly address AI regulation, they remain vital in ensuring that practicable steps are taken to encourage the development and use of AI and other 4IR technologies. While a number of policy documents guide digital heath implementation, no specific legislation addresses software as a medical device.

Within the legal framework for data protection, restrictions on the processing of personal data and the prohibition on automated decision-making are vital in the regulation of AI systems. AI technologies may receive some protection under the Consumer Protection Act as software is included in the provided definition of 'goods'. Furthermore, ICT/E-legislation and a consideration of IP legislation, jurisprudence and soft law may be essential in ensuring that these technologies are used properly.