MALAWI

ACRONYMS

AI	Artificial intelligence
ICT	Information and communication technology
MACRA	Malawi Communications Regulatory Authority
MTA	Material transfer agreement
NHSRC	National Health Sciences Research Committee
PI	Principal investigator
PMPB	Pharmacy, Medicines and Poisons Board

MODES OF INFORMED CONSENT

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

There is no general data protection law. The available law is the Electronic Transactions and Cyber Security Act, although it is not relevant in the context of health research.

Nevertheless, the Genetic Research Guidelines require that genetic analyses be done in the country. Only in exceptional circumstances can genetic resources be exported outside Malawi for analysis. The National Health Research Committee (NHSRC), which does ethical reviews of health research proposals in Malawi, must approve the export in terms of the MTA undertaken by the researcher. The genetic material must not be identifiable at the time of 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, including the right to personal liberty, right to human dignity, right not to be subjected to experimentation without consent, right to participate in culture, and the rights to freedom of association, conscience (including academic freedom), opinion, and expression. The Constitution envisages these rights but they are specified and implemented in legislation, regulations and policy guidelines.

Regulatory and Supporting Institutions

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

- Centre for Social Research
- International Development Research Centre
- Malawi Communications Regulatory Authority
- Medical Council of Malawi
- National Health Research Committee
- National Research Council of Malawi
- Republic of Malawi Ministry of Health.

Individual and Community Benefit Sharing

The approach to benefit sharing is as follows. With respect to research on human participants, there have to be consultations between the investigators and the community before the research starts and such consultation must be continued throughout the study. The investigators have a duty to demonstrate that the research or study contributes to capacity building such as enhancement of local healthcare, the conduct of health research and the ability to respond to

public health needs and how the local community will benefit from the research product(s). The outcome of the research must also be shared with the research participants and the community.

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 and it must take place in an authorised medical facility. All forms of consent for biomedical research must be written unless otherwise stated.

The sale and purchase of human organs or tissues is strictly prohibited. The donor cannot receive payment for such donations except compensation for costs incurred in the process of making the donation or compensation for injuries incurred during scientific research. The amount paid as compensation should not exceed an amount which is reasonably required to cover the costs involved in the importation, export, acquisition or supply of the tissue, gamete, blood or blood product.

The purpose of the donation of human organs, tissues, blood or blood products is limited to educational scientific research, and therapeutic and diagnostic purposes.

(2) Patenting

Patenting of new inventions is permitted and encouraged by the law. However, an application for a patent may be rejected if it is found to be frivolous or the invention is something that is considered to be contrary to well established natural law or if the use of the invention would be contrary to the law or morality.

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.

Studies have reported on the use of geospatial mapping for the improvement of human welfare in Malawi, including in the area of agriculture and healthcare. However, the legal framework for regulating the lawful use of such data is largely absent, and there is no information publicly available on how the Government of Malawi intends to develop legislation, policies or guidelines for the use of GIS data in relation to healthcare services and health research.

In this context there has to be reliance on laws pertaining to data protection in general. Pertinent legislation is discussed below.

General Framework

Legislation

Malawi recently published a Data Protection Bill as discussed below, but does not have any promulgated data protection laws or laws on geospatial data.

Electronic Transactions and Cyber Security Act

This Act covers data protection and privacy. A data controller could process personal data (which includes genetic materials which may identify a person) fairly and legally and for a specific and legitimate purpose. The Act defines personal data as any information relating to an individual who (a) may be directly identified; or (b) if not directly identified, may be identifiable by reference to an identification number or one or several elements related to physical, physiological, genetic, psychological, cultural, social, or economic identity. Furthermore, personal data may be processed only if the data subject has given consent, or if the processing of the personal data is in the interest of the public and the interest of the data subject, or in the event of a legal obligation. The Act defines consent as any freely given specific and informed indication by a data subject of his wishes, by agreement, to his personal data being collected, processed or stored.

The fundamental rights and freedoms of data subjects should, however, always be observed. The Act offers broad protection of all data (including genetic data) which is connected to a data subject.

The Constitution of Malawi

The Constitution contains several sections that pertain to the protection of individual rights, including the right to privacy. It recognises

- the right to personal privacy in terms of protection from inhuman and degrading treatment, which guarantees that every person has the right to respect for his/her dignity and personal privacy;
- protection from unlawful entry, which prohibits unlawful entry into a person's home or other property without consent, except in specific circumstances outlined by law;
- protection of freedom of expression, which acknowledges that freedom of expression should not be used to violate the privacy of individuals.

The Constitution provides a foundation for the protection of privacy and other fundamental rights. However, more specific regulations related to data protection and privacy may be addressed through separate legislation and regulations.

Anatomy Act

This Act further prevents the publication of information which would result in the discovery of the identity of a tissue donor unless the donor has given consent to this publication of information. The Act is more specifically drafted to regulate and protect the human body after death.

When one collectively reviews the Electronic Transactions and Cyber Security Act and the Anatomy Act, their collective provisions provide some level of data protection, although the Anatomy Act is silent on geospatial data.

Access to Information Act

This Act also provides protective measures that one would find in data protection legislation. Personal information about a third party may not be disclosed in terms of the Act as it is deemed to be information exempt from disclosure. The Act defines personal information as:

> information about an identifiable individual including—
> (a) information relating to the race, colour, sex, language, political or other opinion, national, ethnic or social origin, disability, property, birth or other status or condition of the individual;
> (b) information relating to the education, *medical*, or employment history of the individual or information relating to financial transactions in which the individual has been involved;
> (c) any identifying number, symbol or other particular assigned to the individual;
> (d) the address, fingerprints or blood type of the individual;
> (e) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; and
> (f) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual.

The above includes physical address, which directly refers to geospatial data. Geospatial data in this context forms part of personal information and deserves the same protections offered in this Act.

Data Protection Bill

If enacted, this will deal with data protection and related matters. The Bill will not apply to the processing of personal data to the extent that it is carried out by one or more individuals solely for personal, recreational, or household purposes. The Bill provides a comprehensive list of definitions including definitions for personal data, sensitive personal data, biometric data (which includes DNA), personal data breach, and data subject.

Definitions in the Bill

The Bill defines personal data as any information relating to an individual who can be identified or is identifiable, directly or indirectly by reference to an identifier such as a name, an

identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual. Geospatial data, such as location data from which an individual is identifiable, forms part of personal information and deserves the same protections offered in this Bill.

Although the Bill further distinguishes between personal information and sensitive personal information, it is doubtful that geospatial information can be considered sensitive personal information, because it is not listed, defined or referred to in the definition of sensitive personal information. The Bill defines sensitive data as personal data relating to an individual's biometric data; race or ethnic origin; religious or similar beliefs, such as those reflecting conscience or philosophy; health status; sex life or sexual orientation; political opinions; or affiliations. The Bill also includes a 'catch all' for "any other personal data prescribed by the Authority as sensitive personal data pursuant to section 19(2) …".

Exceptions to the consent requirement

These considerations merit special attention by health researchers combining geospatial data with health data in such a way that individuals may be identifiable. The Bill permits processing of sensitive data with consent by the individual, but also contains an exemption for research where the processing is necessary for archiving purposes in the public interest, or for historical, statistical or scientific research. There is an additional exemption for processing sensitive information without consent where the processing is necessary for reasons of public health and it provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. There is also a complete exemption from all the requirements for processing by authorities responding to a public health emergency. These exceptions are made explicit in the Bill and greenlight the use of geospatial data in combination with health data for the specified purposes.

Different roles and definitions for "data controller" and "data controller or data processor of major importance"

All forms of surveillance however have privacy implications and require careful consideration of adequate safeguards. The Bill offers two comprehensive definitions for "data controller" and "data controller or data processor of major importance." Data controller is defined as an individual, private entity, public authority or agency or any other body who or which, alone or

jointly with others, determines the purposes and means of the processing of personal data. Data controller or data processor of major importance is defined as:

> a data controller or data processor that is domiciled, ordinarily resident, or ordinarily operating in Malawi and processes or intends to process personal data of more than 10,000 data subjects who are within Malawi, or a greater number of data subjects prescribed by the Authority in rules published in the Gazette, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Malawi as the Authority may designate.

Schools, universities, or private companies, among many other institutions, may fall into the category of data controller and depending on the volume of data could be considered to be a "data controller or data processor of major importance". This may also apply to the use of geospatial datasets, where they contain personal data (i.e., can be used to identify individuals). If they can be regarded as having a particular significance for the society and economy, such as the geographical prevalence of disease and/or spread of diseases for purposes of managing such spread, the regulation of such data may fall squarely within this ambit. The implication is that registration will then be as a data controller of major importance. The Bill does not indicate what additional/amended regulations may apply to such a controller.

The Bill does not offer a finite definition of what may be considered to be of major importance, and possibly "of major importance" should be deleted "to promote universal data protection". Although the definitions provided are comprehensive, they have been drafted in such a fashion as to include rather than exclude entities, institutions, or organisations.

The above definitions are more comprehensive than the definition of "data controller" provided in the Electronic Transactions and Cyber Security Act: a person who, acting either alone or in common with other persons, determines the purpose for which, and the manner in which, any personal data is processed, or is to be processed and thus controls and is responsible for the keeping and using of personal data, and the term includes a person who collects, processes or stores personal data.

Objectives of the Bill

The objectives of the Bill include:

- promoting digital privacy and data security;
- affording rights to individuals who may have data which is processed;
- implementing standards which must be observed when personal data is transferred out of Malawi.

The Bill also offers a comprehensive section on enforcement which may result in sanctions, fines and even imprisonment being imposed if a data controller or data processor is in violation of the Act (if the Bill is enacted), and offers the possibility of compensation to a data subject who suffers harm as a result of violations committed by the data controller or data processor.

The Data Protection Office

The Data Protection Office is established as a unit in the Data Protection Bill and operating under MACRA (the Authority established in the Bill) has been criticised as the Office would not be able to act independently. It has been suggested that this element of the Bill should be reviewed and an independent authority operating outside of MACRA should be instituted.

Conclusion and Recommendations

Malawi has no laws that specifically deal with geospatial data or data protection. Currently, protection of data privacy and confidentiality can be deduced from the broad interpretation of laws relating to electronic communication and the networks that make communication possible.

CROSS-BORDER SHARING OF DATA

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

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

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 Bill, 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 Bill and to begin to assist users in navigating the Bill. It is not comprehensive, and users of this Bill 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. Malawi does not have a Data Protection Act, but a Data Protection Bill was introduced in 2021. If passed, it will become a general data protection law that will apply to the processing (i.e., use) of personal data in all sectors. Therefore, it will not be a regulation that was introduced to regulate research. However, as research processes vast quantities of personal data, the Data Protection Bill, once passed, will apply to research.

The Data Protection Bill will be one of several laws that must be complied with when transferring data for research.

Health Research Regulations and Cross-Border Data Sharing

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

The relevant national legislation and guidance are (the):

- Constitution of Malawi
- National Policy Measures and Requirements for the Improvement of Health Research Co-ordination in Malawi, 2012. This was published by the National Commission for Science and Technology and relates to Malawi's Science and Technology Act.
- Pharmacy and Medicines Regulatory Authority Act
- Policy Requirements, Procedures and Guidelines for the Conduct and Review of Human Genetic Research in Malawi, 2012
- Public Health Act
- The National Health Research Agenda, 2012.

These documents set out the legal and ethical requirements that must be met for the conduct of research in Malawi. Malawi has strict provisions on the use of genetic material and data in research. Transfer of genetic material (locally or nationally) can take place only if the researcher and the other research group are collaborating on a research study that has been approved by the National Health Sciences Research Committee (NHSRC), if genetic material and information is provided in a form that ensures that participants cannot be identified, and if the research group ensures that privacy and confidentiality are not compromised while holding the material and information.

Cross-border movement of genetic material is not permitted unless there is a justifiable reason to do so, such as to expedite a timely therapeutic cause. In such a case, cross-border

movement of genetic material is not permitted unless prior approval for such a transfer under a material transfer agreement has been reviewed and is signed by the NHSRC. To transfer genetic material, the NHSRC must approve the research study. The application must describe how the privacy and confidentiality of the individuals and communities, as well as the safety of such materials, will be maintained.

Data Protection Bill

In addition to these legal and ethical requirements, the Data Protection Bill, if passed, will apply to the processing of all personal data, but owing to the importance of research, there are special provisions in place for this. Personal data may be processed for inter alia scientific research, and sensitive personal data may be processed for scientific research, but only if one of the conditions for the processing of personal data in the Data Protection Bill has been met – one of which is for scientific research. The conditions set out in the Data Protection Bill must all be met for research. In addition, extra conditions must be met prior to the transfer of personal data across borders.

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

The Main Actors Defined in the Data Protection Bill

	Legal definition	**Layman explanation**
Data subject	An individual to whom personal data relates.	The person to whom the data relates.
Data controller	An individual, private entity, public authority or agency or any other body who or which, alone or jointly with others, determines the purposes and means of the processing of personal 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	An individual, private entity, public authority or agency or any other body who or which processes personal data on behalf of or at the	Someone who is not directly employed by the data controller, but who processes personal data under the direction of the data controller.

	direction of a data controller or another data processor.	They may be a consultant, for example.
Information Regulator	Not defined in the Data Protection Bill.	The independent body established to monitor and enforce compliance with the law.
Information Officer/Data Protection Officer	Not defined in the Data Protection Bill.	An individual in an organisation who is appointed to advise and promote compliance with the law.
Authority	The Malawi Communications Regulatory Authority established under the Communications Act.	

Categories of Data Listed in the Data Protection Bill

	Legal definition	**Layman explanation**
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allow or confirm the unique identification of that individual, including without limitation by physical measurements, facial images, blood typing, fingerprinting, retinal scanning, voice recognition and DNA analysis.	
Personal data	Any information relating to an individual who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual.	Data/information about a particular person that can identify him or her.
Sensitive personal data	Personal data relating to an individual's: (a) biometric data; (b) race or ethnic origin; (c) religious or	Personal data/information about a particular person which is considered sensitive, such as health

	similar beliefs, such as those reflecting conscience or philosophy; (d) health status; (e) sex life or sexual orientation; (f) political opinions or affiliation; or (g) any other personal data prescribed by the Authority as sensitive personal data pursuant to the Bill. The Authority may prescribe further categories of personal data that may be classified as sensitive personal data, further grounds on which they may be processed, and safeguards that may apply, having regard to: (a) the risk of significant harm that may be caused to a data subject or class of data subjects by the processing of such category of personal data; (b) the reasonable expectation of confidentiality attached to such category of personal data; and (c) the adequacy of protection afforded to personal data generally.	data and genetic data, and which receives additional legal protection.
Pseudonymised data/information	This is not defined in the Bill, although 'pseudonymisation' is referred to as relating to measures to ensure the security, integrity and confidentiality of personal data.	Data where the direct identifiers have been removed (e.g., a name) so that it is impossible to identify the person without adding other information. This is often called coded data. Data protection law still applies to pseudonymised data.

If a data controller uses pseudonymisation and de-identification techniques, the data controller is required to regularly test that the measures employed are effective, updated when necessary and that new measures are instituted to address any shortcomings in current methods or to address new risks.

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

- personal data;
- sensitive personal data (including biometric data);

- pseudonymised data; and
- de-identified data.

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

In the absence of a test, the following is recommended from what can be clearly ascertained from the Bill and drawing on the tests in other jurisdictions:

Recommended test - Ask yourself:

1. Is the data able to individually identify a data subject, directly or indirectly, in reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social, or economic identity of that individual?
2. Can the data be linked with other data kept separately, in order to identify a data subject, either directly or indirectly?
3. Is the method employed to de-identify the data subject reversible?
4. Is there any reasonably foreseeable method that could be used by someone to identify the data subject directly or indirectly, by employing methods such as linking it to other data, or manipulating the data, or any other novel methods?

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

Special Note Regarding Genetic and Genomic Data

DNA analysis is considered sensitive personal data. It has a higher level of protection under data protection law. There is ongoing debate about whether genomic datasets can ever truly be

considered not to be personal data, in particular as genetic data is an identifier. Therefore, special care must be taken in deciding whether a genomic dataset can be considered to fall outside of the definition of personal data. Therefore, consider whether your data allows for anyone to identify the data subject.

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

1. *Lawfulness of data processing:* Personal data must be processed lawfully, fairly, and transparently in relation to the data subject. The processing of sensitive personal data is generally not permitted unless it falls within one of the grounds in the Bill.
2. *Provision of information:* When collecting personal data directly from a data subject, the data controller must provide the data subject with the identity and contact details of the data controller, the basis of processing and the purposes for which the processing of personal data is intended, information on the third parties which the data will be shared with, the rights of the data subject, and the right to lodge a complaint with the Authority. When personal data is not collected directly from the data subject, the data controller must abide by the provisions in the Bill, unless the data subject already has such information or providing such information is impossible or would involve a disproportionate effort or expense.
3. *Purpose specification:* Personal data should be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
4. *Data minimisation:* Only the data that is necessary for the specific purpose should be collected and processed. It is essential that the personal data is adequate, relevant, and limited only to the amount of data that is required to achieve the objectives for the collection or further processing of the personal data.
5. *Retention:* Personal data should not be retained for longer than is necessary to achieve the purpose of collection or further processing except where retention is required by law, or where the data subject consents to the retention.
6. *Accuracy:* Personal data must be accurate, complete, not misleading and, where necessary, kept up to date in terms of the purpose for which the personal data was collected.
7. *Obligations of data controller and data processor:* Personal data should be processed in a manner that ensures appropriate security, including protection against unauthorised or

unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Both organisational and technical measures must be put in place to secure the data.

Data Subject Rights in Terms of the Data Protection Bill

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

1. *Right to information:* The data subject has the right to be told whether the data controller, or a data processor operating on its behalf, is storing or otherwise processing personal data relating to the data subject and also about the source of such personal data.
2. *Right to access:* The data subject has the right to obtain a copy of the personal data, in electronic format, that the data controller has in his/her possession. The exception is when providing the data would lead to an unreasonable cost for the data controller, in which case the data subject may be required to bear some or all of the costs.
3. *Right to correction:* The data subject has the right to have incorrect personal data corrected. Where this is not feasible or unsuitable, the data subject has the right to have inaccurate, outdated, incomplete, or misleading personal data deleted.
4. *Right to deletion:* The data subject has the right to have any personal data deleted, which the data controller is not entitled to retain.
5. *Right to withdraw consent:* The data subject has the right, at any time, to withdraw consent for the processing of his/her personal data.
6. *Right to object:* The data subject can object to the processing of his/her personal data where the lawful basis of processing is not consent.
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.
8. *Right to data portability:* The data subject has the right to receive personal data about him/her from a data controller, to transmit personal data to another data controller, and to move his/her data from one data controller to another.

Cross-Border Transfer of Personal Data

When considering cross-border transfers of data for research, all the provisions of the Data Protection Bill must be met. The Bill also has a number of provisions on cross-border transfers of personal data that, in addition to the other provisions, must be met.

Cross-border transfers of personal data are not explicitly defined in the Data Protection Bill. However, this would occur when personal data is being sent from a data controller or data processor in Malawi to a data controller in another country. It *could* also include a situation where a researcher outside of Malawi accesses the personal data inside the country. It *could* also include putting data onto a cloud where the server is not hosted in the country. However, this is not yet settled law.

Grounds for the cross-border transfer of personal data

In addition to meeting the provisions set out in the law, there must be a ground under which the cross-border transfer of personal data can take place. These grounds are:

1. *Basis for cross-border transfer of personal data:* The recipient of the personal data is subject to a law, binding corporate rules, contractual clauses, code of conduct or certification mechanism that affords an adequate level of protection with respect to the personal data.
2. *Adequacy of protection:* A level of protection is adequate if it upholds principles that are substantially similar to the conditions for processing personal data provided for in the Data Protection Bill. In considering whether the protection is adequate, there must be consideration of the following:
    a. the availability of data subject rights, the ability of data subjects to enforce their rights, and the rule of law;
    b. any legally binding instrument between the Authority and a public authority in the recipient country addressing elements of adequate protection;
    c. access of a public authority to personal data;
    d. the existence of an effective data protection law;
    e. the existence and functioning of an independent data protection supervisory authority; and
    f. international conventions that are binding on the country and membership of any multilateral or regional organisations.

The Authority may give notice in the Gazette of any country, region or specified sector in a country, or standard contractual clauses that it has determined (and also not determined) as affording or as not affording an adequate level of protection. The Authority may approve binding corporate rules, codes of conduct, or certification mechanisms proposed to it by a data controller, where the Authority determines that they have adequate protection. The Authority can make a decision here based on a decision made by other data protection authorities where their decision took into account the same factors as required by the Data Protection Bill. Researchers are therefore encouraged to first consult the Gazette to see if the cross-border transfer of personal data could fall under this adequacy provision.

3. *Other bases for transfer of personal data:* Without adequacy, personal data can be transferred outside Malawi, only if the:
   a. data subject has given, and not withdrawn, consent to the transfer and has been informed of the possible risks resulting from a lack of adequate protection;
   b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
   c. transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and a third party; or
   d. transfer is for the benefit of the data subject and it is not reasonably practicable to obtain the consent of the data subject, and if it were reasonably practicable to obtain such consent the data subject would likely give it.

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

In Malawi, there is no specific legislation on AI or legislation that addresses AI-related issues, including predictive algorithms. It is therefore necessary to consider the legal landscape of 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 is no technological provision, industry- or sector-specific guidance in place.

Digital Health/E-Health

The National Digital Health Strategy 2020–2025 guides digital health in Malawi. The Medical Council of Malawi established by the Medical Practitioners and Dentists Act regulates health professionals. The Code of Ethics Medical Council of Malawi sets out the code of practice for health professionals.

There are guidelines and codes of ethics which regulate medical research in Malawi:

- National Guidelines for the Conduct of Health Research in Malawi
- National Health Sciences Research Committee
- Procedures and guidelines for the conduct of health-related research in Malawi.

There is no specific regulation for medical devices that use AI. The Pharmacy and Medicines Regulatory Authority Act, through the Pharmacy, Medicines and Poisons Board (PMPB), regulates medical devices in Malawi.

Consumer Protection & ICT/E-Legislation

Consumer Protection	• Consumer Protection Act
ITC/E-Legislation	• Electronic Transactions and Cyber Security Act

Data Protection Law

There are no data protection laws, but the Electronic Transactions and Cyber Security Act contains provisions usually associated with data protection laws.

The Act covers data protection and privacy. A data controller should process personal data (which includes genetic materials which may be identified to a person) fairly and legally and for a specific and legitimate purpose. Furthermore, personal data may be processed only if the data subject has given consent, or if its processing is in the interest of the public and the interest of the data subject, or in the event of a legal obligation. However, the fundamental rights and freedoms of data subjects should always be observed. The Act offers a broad protection of all data (including genetic data) connected to a data subject.

The Anatomy Act further prevents the publication of information which would result in the discovery of the identity of a tissue donor unless the donor has given consent to this publication of information. The Anatomy Act is more specifically drafted to regulate and protect the human body after death.

The collective provisions of the Electronic Transactions and Cyber Security Act and the Anatomy Act provide some level of data protection. In furtherance of this, the Access to Information Act also provides protective measures. Personal information about a third party may not be disclosed in terms of the Access to Information Act, as personal information is deemed to be information exempt from disclosure.

Data Protection Bill

Although the above Acts provide some measure of data protection, the Data Protection Bill will deal with data protection and related matters. The Bill provides a comprehensive list of definitions, including definitions for 'personal data', 'sensitive personal data', 'biometric data' (which specifically includes DNA), 'personal data breach' and 'data subject'. It will also regulate the cross-border transfer of personal data. Data may only be transferred outside of Malawi if the recipient of the data is subject to laws, rules and regulations that provide an adequate level of data protection that is on a par with the level of protection afforded in the Data Protection Bill.

There is a prohibition on automated decision-making. A data subject must not be subject to a decision which is based solely on the automated processing of his/her personal data, except in instances where it is: necessary for the execution of a contract, authorised by a written law, or authorised by the consent of the data subject.

Objectives of Data Protection Bill and enforcement measures

The objectives of the Data Protection Bill include promoting digital privacy and data security, affording rights to individuals who may have data which is processed, and implementing standards which must be observed when personal data is transferred outside of Malawi. Furthermore, the Bill offers a comprehensive section on enforcement which may result in sanctions, fines and even imprisonment if a data controller or data processor violates the Act (if the Bill is enacted) and offers the possibility of compensation to a data subject who suffers harm as a result of violations committed by the data controller or data processor.

Intellectual Property

Copyright Act

The Malawi Copyright Act deals with technological and legal developments.

National Intellectual Property Policy

The National Intellectual Property Policy is part of the Malawian government's Growth and Development Strategy III, which has identified industrialisation and the structural transformation of the economy as a key priority area essential for maintaining long-term growth and economic development. The Policy acknowledges that intellectual property has

been sidelined from the national development agenda since Malawi's independence, recognises that intellectual property is a catalyst for technologic advancement, economic growth and national development, and provides a framework to foster the generation, protection and exploitation of intellectual property. While Malawi has intellectual property laws, these (except for the Trademarks Act and Copyright Act) were inherited from its former colonial power, the United Kingdom, and are outdated.

Intellectual property is administered by two separate institutions:

- *Industrial property* (patents, designs and trade marks) is administered by the Department of the Registrar General which falls under the Ministry of Justice
- *Copyright* is administered by the Copyright Society of Malawi which falls under the Ministry responsible for Culture.

The National Intellectual Property Policy aims to address the deficiencies created by these outdated intellectual property laws and the antiquated institutions that administer and manage them, as well as the lack of deliberate and coordinated policies aimed at leveraging the intellectual property system as a tool for stimulating the generation, protection and commercialisation of intellectual property assets.

Five priority areas of the National Intellectual Property Policy:

1. *An effective institutional framework for modernising the administration of intellectual property rights*. The Policy envisages the creation of a modern, unified and autonomous agency responsible for the administration and management of intellectual property in Malawi.
2. *The generation and protection of intellectual property assets.* The Policy acknowledges that the output of locally generated intellectual property rights is extremely low and envisages the stimulation of such rights through the provision of various types of incentives and funding.
3. *The effective exploitation and commercialisation of intellectual property assets.* The Policy envisages, among other things, the creation of innovation centres or units and support structures for micro, small and medium enterprises.

4. *An effective and balanced legal regime for intellectual property rights.* The policy envisages a review of patent, copyright and design legislation, the preparation of legislation and strategies for the protection and exploitation of traditional knowledge, genetic resources and expressions of folklore originating from Malawi, and the implementation of international agreements to promote the national interest.
5. *Intellectual property awareness creation and capacity-building.* The policy envisages the teaching of intellectual property at school and tertiary level, the establishment of an Institute of Intellectual Property Attorneys, the development of capacity for intellectual property enforcement and dispute resolution, and the coordination of intellectual property enforcement activities.

The Policy also identifies various stakeholders that are responsible for the implementation of each of these priority areas and provides time frames for their implementation and a monitoring and evaluation plan.

Summary and Analysis

Malawi does not have any strategy/policy instruments related to AI regulation. While several policy documents guide digital heath implementation, no specific legislation provides for AI use in medical devices. The above-mentioned policy documents are interoperable and do not supersede one another. However, relevant provisions found in promulgated legislation take precedence over other regulatory/policy documents. In addition, there is no data protection legislation. However, the Electronic Transactions and Cyber Security Act and the Anatomy Act read together do provide some level of data protection, although this is not extensive. The Data Protection Bill may offer more extensive protections to data subjects, especially the prohibition on automated decision-making.

The Consumer Protection Act provides for safeguards against harmful technologies and provides for recall of such products where they are considered a risk to public health. In addition, ICT/E-legislation, such as the Electronic Transactions and Cyber Security Act and a consideration of intellectual property legislation, jurisprudence and soft law may be essential in ensuring that these technologies are utilised properly.