GHANA

ACRONYMS

AFRO	African Regional Office
AI	Artificial intelligence
ARIPO	African Regional Industrial Property Organisation
CERSGIS	Centre for Remote Sensing and Geographic Information Services Ghana
CSIR	Council for Scientific and Industrial Research
DPA	Data Protection Act
ECOWAS	Economic Community of West African States
GAEC	Ghana Atomic Energy Commission
GCAA	General Civil Aviation Authority
GDPR	General Data Protection Regulation (Europe)
GERMP	Ghana Environmental Resource Management Project
GIS	Geographical information system
GSSTI	Ghana Space Science and Technology Institute
HSMTDP	Health Sector Medium Term Development Plan
ICT	Information and communication technology
IDSR	Integrated disease surveillance and response
MESTI	Ministry of Environment, Science, Technology and Innovation
PCT	Patent Corporation Treaty
PI	Principal investigator
WHO	World Health Organization
WIPO	World Intellectual Property Organization

MODES OF INFORMED CONSENT

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

The main legislation for the protection of personal data is the Data Protection Act (2012). Scientists involved in health research must comply with its provisions.

The Ghanaian Public Health Act also imposes an obligation on scientific researchers to freely obtain voluntary written informed consent prior to a clinical trial, and participants must be informed of: (i) the aims and objectives of the trial and the way in which it will be conducted; and (ii) the possible risks and adverse effects that may result.

Data Protection Act

Definitions of personal data and genetic data

When a scientist is processing personal data, the provisions of the Data Protection Act apply. The Act defines personal data as data about an individual who can be identified: (a) from the data; or (b) from the data or other information in the possession of, or likely to come into the possession of, the data controller. Genetic data is not defined, but can be located in the special personal data category, which includes the physical, medical, mental health condition or DNA of the data subject.

Exceptions to ban on processing personal data

Scientists may not process personal data without the prior consent of the data subject. Exceptions include: where the processing of data is necessary for the purpose of a contract to which the party is subject; the processing is authorised by law; the processing is required to protect a legitimate interest of the data subject; processing is necessary for the proper performance of a statutory duty;

and where it is necessary to pursue the legitimate interest of the data controller or a third party to whom the data is supplied.

Objections to data processing and preventing data processing

A data subject can object to the processing of his/her personal data. When this happens, the person processing the personal data must stop doing so. A data subject also retains the right to prevent processing of personal data if it causes or is likely to cause him/her unwarranted damage or distress.

Retention of records

The retention of records is not permitted for longer than is necessary to achieve the purpose for which the data was collected and processed, unless, among other things, the data subject consents. Data retained for historical, statistical or research purposes is not included in this requirement.

Exceptions to required consent for processing special personal data

The obligation to gain consent from data subjects extends to special personal data but sometimes this can be overlooked when the processing is necessary for the protection of the vital interests of the data subject. For example, where (a) it is impossible for consent to be given by or on behalf of the data subject; (b) the data controller cannot reasonably be expected to obtain the consent of the data subject; or (c) consent by or on behalf of the data subject has been unreasonably withheld.

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 in the Constitution. These include the right to protection of human dignity, freedom of expression, freedom of thought, and academic freedom. These rights are generally pronounced in the Constitution and are further provided for in legislation, regulations and policy guidelines.

Regulatory and Supporting Institutions

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

- Council for Scientific and Industrial Research
- Ghana Food and Drugs Authority
- Institutional Ethics Committee
- Ministry of Health
- Science and Technology Policy Research Institute.

Individual and Community Benefit Sharing

The approach to benefit sharing is as follows. For research concerning human participants, the research participant must be informed of the expected and potential benefits of the research during and after the research, whether there are any incentives given to participation, and the availability of beneficial products or post-research interventions. Investigators must conduct an assessment and provide research participants with the purpose of the research, procedures, risks and

discomforts, benefits, compensation, confidentiality, voluntariness and the identity of contact persons.

The law does not mention community benefit sharing.

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 such donation is done on a voluntary and non-remunerated basis. Therefore, organs, blood, blood products and gametes cannot be sold in Ghana and a donor cannot receive any payment for such donations. However, the donor is entitled to receive compensation for costs incurred while making the donation. The donor or research participant is also to be compensated for injury sustained during research. A person is not entitled to remuneration in relation to donation of their human biological data.

Purpose is limited to:

- Training of students in health sciences
- Health research
- Advancement of health sciences
- Therapeutic purposes, including the use of tissue in any living person
- Production of therapeutic, diagnostic or prophylactic substances.

Where a research participant is illiterate or cannot sign a written consent form, the document may be explained verbally so there can be consent in another format which is witnessed by an impartial third party who then signs the consent form. Where the participant is a child who cannot understand the study, their signature of assent and that of their legal guardian are required. The following information must be included in the consent form:

- Description of any reasonably foreseeable risks or discomforts to the subject.
- Description of any benefits to the subject or to others that may reasonably be expected from the research, including payment or free treatment.
- Disclosure of appropriate alternative procedures or courses of treatment, if applicable, which may be advantageous to the subject.
- A statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained.

(2) Patenting

Patenting new inventions in Ghana is permitted and encouraged. For an invention to be patented, it must be new, must have involved inventive steps and must be industrially applicable. However, several inventions are excluded from patenting. These include: discoveries and scientific theories, and methods for treating or diagnosing humans or animals and inventions whose commercial exploitation would be detrimental to the public order or morality – including human, animal and plant life or health. 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, guidelines and policies are discussed below.

Legal clarity on the use of persons' geospatial data for public health surveillance in Ghana is provided. The privacy risks brought about by novel geospatial technologies are analysed and legal clarity is provided on how to comply with the law. The extant legal requirements for using persons' geospatial information for public health surveillance in Ghana are analysed and spaces for policy improvement are identified.

General Framework

Legislation

The Electronic Transactions Act

The Act prohibits the following activities on the internet: unsolicited communications; unauthorised access to electronic records, electronic systems or computers; unauthorised access to an electronic communication service facility; unauthorised modification of a program or electronic record; fraud, misrepresentation and forgery involving an electronic medium; fraudulent advertisements; and maliciously causing damage to a computer.

The Electronic Communications Act

The Act prohibits the circulation of false information:

A person who knowingly gives false or misleading information to the Authority commits an offence and is liable on summary conviction to a fine of not more than one thousand penalty units or to a term of imprisonment of not more than three years or to both.

In terms of the above clause, false information damaged or retarded the management of health emergency services and efforts during the Covid-19 pandemic and if false information is also applied to geospatial information this may prevent management from adequately detecting, observing and predicting the spread of diseases.

False signals

A person who knowingly transmits or circulates false or deceptive distress, safety or identification signals commits an offence and is liable on summary conviction to a fine of not more than three thousand penalty units or to a term of imprisonment of not more than five years or both.

False communications

(1) A person who by means of an electronic communications service, knowingly sends a communication which is false or misleading and likely to prejudice the efficiency of life saving service or to endanger the safety of any person, ship, aircraft, vessel or vehicle commits an offence and is liable on summary conviction to a fine of not more than three thousand penalty units or to a term of imprisonment of not more than five years or both.

(2) A person is taken to know that a communication is false or misleading if that person did not take reasonable steps to find out whether the communication was false, misleading, reckless or fraudulent.

(3) Subsection (2) does not apply to the operator or provider of a network or service over which a communication is sent.

Constitution of the Republic of Ghana

The Constitution provides that no person be subjected to interference with the privacy of his/her home, property, correspondence or communication, except in accordance with the law and as may be necessary in a free and democratic society for public safety or economic well-being of the

country, for the protection of health, or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others. Ghana also provides for the protection of privacy in its common law which is recognised by the Constitution as a source of law in Ghana. The common law of Ghana consists of the rules of law generally known as the doctrines of equity and the rules of customary law, including those determined by the Superior Court of Judicature. Although the Data Protection Act (DPA) provides for Regulations (legislative instruments) and executive instruments for the implementation of the law, no such instrument has been issued. The Data Protection Commission has provided guidelines for the registration of data controllers and data processors.

Data Protection Act

The Act covers the public and private sector processing of personal data. Data controllers and data processors are both widely defined:

> *data controller* means a person who either alone, jointly with other persons, or in common with other persons, or as a statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed;
> *data processor* in relation to personal data means any person other than an employee of the data controller who processes the data on behalf of the data controller.

Consent, justification and objection: (1) A person must not process personal data without the prior consent of the data subject unless the purpose for which the personal data is processed is (a) necessary for the purpose of a contract to which the data subject is a party; (b) authorised or required by law; (c) to protect a legitimate interest of the data subject; (d) necessary for the proper performance of a statutory duty; or (e) necessary to pursue the legitimate interest of the data controller or a third party to whom the data is supplied. (2) Unless otherwise provided by law, a data subject may object to the processing of personal data. (3) Where a data subject objects to the processing of personal data, the person who processes the personal data must stop processing the personal data.

Right to prevent processing of personal data: (1) An individual must at any time by notice in writing to a data controller require the data controller to cease or not begin processing for a specified purpose or in a specified manner, personal data which causes or is likely to cause unwarranted damage or distress to the individual. (2) A data controller must within 21 days after receipt of a notice inform the individual in writing (a) that the data controller has complied or intends to comply with the notice of the data subject, or (b) of the reasons for non-compliance. If the identification of someone's physical location causes unwarranted damage or distress, this could lead to a person giving written notice to cease data processing.

The DPA distinguishes between personal data and special personal data.

The term *personal data* means data about an individual who can be identified (a) from the data, or (b) from the data or other information in the possession of, or likely to come into the possession of, the data controller.

This 'other information' may include geospatial data which could lead to the identification of an otherwise unidentified person or group of persons. People living in remote rural villages may often be identified as a group or a certain tribe based on the location where they live. This may have privacy implications.

Special personal data

The term *special personal data* means personal data which consists of information that relates to: (a) the race, colour, ethnic or tribal origin of the data subject; (b) the political opinion of the data subject; (c) the religious beliefs or other beliefs of a similar nature of the data subject; (d) the physical, medical, mental health or mental condition or DNA of the data subject; (e) the sexual orientation of the data subject; (f) the commission or alleged commission of an offence by the data subject; or (g) proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in the proceedings. The Act distinguishes between personal information and special personal data, but it is doubtful that geospatial information can be considered as special personal data, because it is not listed, defined or referred to in the definition of special personal data.

Prohibition of processing of a defined list of special data

The DPA prohibits processing of a defined list of special personal data unless additional protections are in place. This relates to (a) a child who is under parental control in accordance with the law, or (b) the religious or philosophical beliefs, ethnic origin, race, trade union membership, political opinions, health, sexual life or criminal behaviour of an individual.

Consent and research exemption

These considerations merit special attention by health researchers combining geospatial data with health data in such a way that individuals can be identifiable. The DPA permits processing of special personal information with consent by the individual. It does not contain a general exemption for research. However, two provisions could be relied on by health researchers requiring an exemption from the requirement to obtain informed consent from each individual:

> Special personal data shall not be processed unless the processing is necessary for the protection of the vital interests of the data subject where:
> (a) it is impossible for consent to be given by or on behalf of the data subject,
> (b) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
> (c) consent by or on behalf of the data subject has been unreasonably withheld.

This could apply during health emergencies. All forms of surveillance have privacy implications and require careful consideration of adequate safeguards.

Processing of special personal data for medical purposes

In relation to health research generally, the DPA provides that the processing of special personal data is presumed to be necessary where it is required for medical purposes and the processing is undertaken by a health professional, and pursuant to a duty of confidentiality between patient and health professional. 'Medical purposes' includes the purposes of preventive medicine, medical diagnosis, *medical research*, provision of care and treatment and the management of healthcare services by a medical or dental practitioner or a legally recognised traditional healer.

Automatic processing of geospatial data

Processing of geospatial data often takes place automatically when automatic means such as artificial intelligence are used to link the data to an individual. Where such personal data will be used to make decisions that have a 'significant' effect on that individual, the processing must not be made 'solely' by automatic means without notifying the individual and providing him/her a mechanism to challenge the decision.

Guidelines and Policies

Technical guidelines for Integrated Disease Surveillance and Response (IDSR)

These were adapted from an original document developed by the World Health Organization (WHO)/African Regional Office (AFRO) and the US Centers for Disease Control and Prevention.

General Rules for Flying a Drone in Ghana

The most important rules for flying a drone in Ghana are:

- All drones must be registered with the General Civil Aviation Authority (GCAA). Registration fees may cost up to $4,000, and failure to register a drone can result in a 30-year prison term.
- Do not fly within 10 kilometres (6 miles) of airports or helipads or higher that 400 feet vertically.
- Visual line of sight must be maintained with drones.
- Drone insurance is required.
- Drones may only be operated at night with a special permit from the GCAA.
- Drones may not fly in restricted areas.
- Goods may not be dropped or transported via drone without prior special authorisation.
- A drone operator must be at least 18 years of age.
- Drones may not be operated in congested areas of cities, towns, or settlements, and may not be flown over crowds.

- Drones may not fly within a 30 metre (98 feet) radius of buildings or vehicles without prior permission.

The above may have implications for personal data privacy in terms of the DPA.

National E-Health Strategy, 2010

In July 2010, the Government of Ghana launched the national e-Health strategy. The key strategies are to streamline the regulatory framework for health data and information management, building sector capacity for wider application of e-Health solutions in the health sector, increasing access, and bridging the equity gap in the health sector through the use of ICT, and moving towards a paperless records and reporting system.

Definition of e-Health

Any definition of e-Health should encompass the full spectrum of ICTs while appreciating the context of use and the value they bring to society. Pagliari et al.[1] defined e-Health as:

> an emerging field of medical informatics, referring to the organisation and delivery of health services and information using the internet and related technologies. In a broader sense, the term characterises not only a technical development, but also a new way of working, an attitude, and a commitment for networked, global thinking, to improve healthcare locally, regionally and worldwide by using information and communications technology.

Implementation of the e-Health strategy

The implementation of the e-Health strategy is driven jointly by the Ministry of Communication, Ministry of Health, and other relevant stakeholders. Ghana's e-healthcare service proposal is aimed at the establishment of a National Healthcare Data Centre, which brings together the functions of Health Information Management and Disease Surveillance as a 24-hour comprehensive data centre, which will also serve as an early warning system for the health sector.

[1] Pagliari C, Sloan D, Gregor P, Sullivan F, Detmer D, Kahan JP, Oortwijn W, MacGillivray S. What is eHealth (4): A scoping exercise to map the field. *J Med Internet Res*. 2005;7(1).

This proves how valuable geospatial data is as health emergencies can be much more efficiently managed.

The proposal aimed to connect institutions into a single network under the Ministry of Health, including all hospitals, clinics and health centres across the country and all agencies. This includes the installation of an Electronic Medical Records System and a Patient Management System to streamline the admission, discharge and transfer processes, which are integrated with the claims management system of the National Health Insurance Scheme. It also enables the operation of a Real-Time Bio-surveillance System. Collection and inclusion of geospatial data into this surveillance system may be valuable.

Ministry of Health, Health Sector ICT Policy and Strategy

The Ghana National Health policy and the Health Sector Medium Term Development Plan (HSMTDP 2018–2021 and earlier ones) are all geared towards ensuring Universal Health Coverage and strengthening the health system to respond effectively to the health needs of its citizens, including health emergencies. Consequently, there have been enormous efforts in the expansion of healthcare infrastructure, social health insurance coverage, and the training and employment of the health workforce. The national e-Health strategy aims to streamline the regulatory framework for health data and information management.

Centre for Remote Sensing and Geographic Information Services Ghana (CERSGIS)

CERSGIS began as a Remote Sensing Laboratory with the aim of teaching and conducting research. Under the Ghana Environmental Resource Management Project (GERMP), the Laboratory was commissioned by the Environmental Protection Agency to produce current land use information under the Environmental Information System Development component. The status of the laboratory was then upgraded to the Remote Sensing Applications Unit. The mandates were to produce a national digital map of current land use, with accompanying bulletins for each administrative region, using satellite image data. They were also tasked with developing the capacity to offer remote sensing and GIS services. This may have the potential for the surveillance of and management of future health emergencies. The principal focus of CERSGIS is management of geographic information for sustainable development planning.

Ghana Space Policy and Implementation Plan

The Ghana Space Science and Technology Institute (GSSTI) is a statutory organisation under the Ghana Atomic Energy Commission (GAEC) of the Ministry of Environment, Science, Technology and Innovation (MESTI). GSSTI has the responsibility to harness, coordinate, research, commercialise and explore space science and technology for the socio-economic development of Ghana. It has established three research centres of excellence in (1) Radio Astronomy and Astrophysics, (2) Remote Sensing and Climate, and (3) Satellite Communications and Engineering.

Ghana does not have a space law. In 2022, it adopted a national Space Policy and Implementation Plan to provide a framework for sustainable development using space science and technology. The policy, which will coordinate how ministries, departments and agencies access and consume space data, will help develop the space sector in Ghana. In terms of the policy, GSSTI will be transformed into a space agency and will lead efforts to advance space science and develop the necessary human capital and infrastructure.

Conclusion and Recommendations

Ghana has begun the process of developing applications for the use of spatial information in the field of health. Ghana'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 geospatial data and Ghana has not enacted space laws to regulate and coordinate the optimal use and protection of geospatial data.

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 DPA. 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 in force. It is a general data protection law that applies to the processing (i.e., use) of personal data in all sectors. Therefore, it is not a regulation that was introduced to regulate research. However, as research

processes vast quantities of personal data, the Data Protection 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 this national law, several international treaties and conventions have been signed. Of importance in this domain are the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) and the Supplementary Act A/SA. 1/01/10 on Personal Data Protection within ECOWAS (the ECOWAS Data Protection Act). Ghana has ratified the Malabo Convention.

The relevant national legislation and guidelines are the:

- Public Health Act
- Council for Scientific and Industrial Research (CSIR) Act
- Standard Operating Procedures of CSIR Institutional Review Board

These set out the legal and ethical requirements that must be met for the conduct of research in Ghana. They set no additional requirements to be met in the cross-border flow of data for research.

Data Protection Act

In addition to these legal and ethical requirements, the Data Protection Act applies to the processing of all personal data. However, because of the importance of research, special provisions are in place for research. The conditions 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 this Act are discussed below. This is not a thorough assessment of the Data Protection 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 data for research.

The Main Actors Defined in the Data Protection Act

	Legal definition	Layman explanation
Data subject	An individual who is the subject of personal data.	The person to whom the data relates.
Data controller	A person who either alone, jointly with other persons or in common with other persons or as a statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed.	The person who decides what the data will be used for in research. Legal responsibility falls on the PI *and* on the research institution (as employer).
Data processor	In relation to personal data, any person other than an employee of the data controller who processes the data on behalf of the data controller.	Someone who is not directly employed by the data controller but who processes personal data under the direction of the data controller. The person may be a consultant, for example.
Data Protection Commission	The Commission established under the DPA.	The independent body established to monitor and enforce compliance with the law.
Data supervisor	A professional appointed by a data controller in accordance with the Act to monitor the compliance by the data controller in accordance with the provisions of the DPA.	An individual in an organisation who is appointed to advise and promote compliance with the law.
Foreign data subject	Data subject information regulated by laws of a foreign jurisdiction that is sent into Ghana from a foreign jurisdiction wholly for processing purposes.	
Health professional	A registered medical practitioner or a recognised traditional healer or any person who is registered to provide health services under any law for the time it is in force.	
Recipient	A person to whom data is disclosed including an employee or agent of the data controller or the data processor to whom data is disclosed while processing the data for the	

	data controller. However, it does not include a person to whom disclosure is made with respect to a particular inquiry pursuant to an enactment.	
Third party	In relation to personal data, a person other than (a) the data subject, (b) the data controller, or (c) any data processor or other person authorised to process data for the data controller or data processor.	

Categories of Data Listed in the Data Protection Act

	Legal definition	**Layman explanation**
Personal data	Data about an individual who can be identified: (a) from the data, or (b) from the data or other information in the possession of, or likely to come into the possession of, the data controller.	Data about a particular person that can identify him or her.
Special personal data	Personal data which consists of information that relates to (a) the race, colour, ethnic or tribal origin of the data subject; (b) the political opinion of the data subject; (c) the religious beliefs or other beliefs of a similar nature, of the data subject; (d) the physical, medical, mental health or mental condition or DNA of the data subject; (e) the sexual orientation of the data subject; (f) the commission or alleged commission of an offence by the individual; or (g) proceedings for an offence committed or alleged to have been committed by the individual, the disposal of such	Personal data about a particular person, such as health data and genetic data, and which receives additional legal protection.

	proceedings, or the sentence of any court in the proceedings.	

Data protection law, in general, applies only to personal data. Data that was once personal, in that the data subject could be identified either directly or indirectly from the data, can be made no longer individually identifiable through anonymisation, de-identification or pseudonymisation. Non-personal information is shared more easily, as the data controller no longer needs to comply with the gambit of stringent data protection laws.

To determine whether the data you are sharing is no longer individually identifiable, it is important to make an assessment. This can, however, be challenging. Unfortunately, the Data Protection Act does not define or use the terms anonymisation, de-identification or pseudonymisation, nor is there guidance from the Regulator on these points.

In the absence of direction from the Regulator on a test, the data controller will need to decide. In making this decision, some general points are pertinent (many of which come from guidance related to anonymisation under the EU GDPR):

- An assessment must be made on a case-by-case basis, considering the particular context.
- The anonymisation must be irreversible.
- The assessment is made on the current state of the art. As technology progresses, data that was once deemed to be anonymous may become personal data and thus fall under data protection regulations.
- Consider all means of identification that could be used by a person, for example, available datasets.
- Consider objective factors that are *reasonably likely* to be used, such as technology, resources and time, for identification.
- Possibly 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 sensitive data. It not only falls under the data protection law but also has a higher level of protection.

- There is ongoing debate about whether genomic datasets can ever be rendered truly anonymised, particularly as genetic data is an identifier. In considering whether a genomic dataset can be considered anonymised, the context matters, such as the objective factors relating to the data.

There is uncertainty about whether nobody should be able to individually identify a data subject from the dataset, or whether merely the holder of the data must be unable to do so – in order for it to be considered non-personal or anonymised, such that it falls outside the ambit of data protection laws.

There are two possibilities for the test that data would need to apply to:

(1) Is there anyone in the world who can identify the data subject from the data? (This is an objective test that this context-agnostic, as it is not limited to the circumstances of the data recipient).
(2) Can a specific holder of the data identify the data subject from the data? (This is a context-specific objective test since we consider only whether the specific data holder is able to identify the data subject.)

The context-agnostic test would play out as follows: if Data Controller A sends a pseudonymised dataset (i.e., Data Controller A has the necessary information to identify the people in the dataset) to Controller B, the dataset would never be considered anonymous, as Data Controller A would be able to re-identify the dataset, and therefore there would be someone in the world who could identify the data subject.

The context-specific test would play out differently: 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 considered anonymous in the hands of Data Controller B if Data Controller B did not have access to the identifying dataset and there was no reasonably foreseeable method that could enable him/her to identify the data subject. The test will assess

whether the dataset is anonymous *in the hands of Data Controller B*. It does not matter that Controller A is able to identify the data subject.

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

1. *Accountability:* This is not defined but is required. Generally, under data protection law, this will include keeping a record of processing activities and demonstrating compliance.
2. *Lawfulness of processing:* Personal data must be processed without infringing the privacy rights of the data subject, and must be done lawfully and reasonably. In addition, the data controller or data processor processing the personal data of foreign data subjects must ensure that personal data is processed in compliance with data protection legislation of the foreign jurisdiction from which the personal data originated.
3. *Specification of purpose:* Personal data must be collected only for a purpose which is specific, explicitly defined and lawful and which is related to the functions or activity of the person. A data controller who collects data must take the necessary steps to ensure that the data subject is aware of the purpose for the collection of the data.
4. *Compatibility of further processing with purpose of collection:* Where a data controller holds personal data collected in connection with a specific purpose, further processing of the personal data must be for that specific purpose.
5. *Quality of information:* A data controller who intends to process personal data must ensure that the data is complete, accurate, up to date and not misleading, having regard to the purpose for the collection or processing of the personal data.
6. *Openness:* This is not defined but is required. Generally, under data protection law, this requires providing a data subject with information on the processing of his/her personal data.
7. *Data security safeguards:* A data controller must take the necessary steps to secure the integrity of personal data in the possession or control of a person through the adoption of appropriate, reasonable, technical and organisational measures to prevent loss, damage or unlawful access.
8. *Data subject participation:* This is not defined but is required.

Data Subject Rights in Terms of the Data Protection Act

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

(1) *Right to access:* The data subject has a right to request a data controller to confirm whether the data controller holds personal data about the data subject. This includes the right to request a data controller to give a description of the personal data which is held by a third party including the identity of all third parties with access to the information of the data subject.
(2) *Right to correct personal data:* The data subject may request the data controller to correct or delete personal data about the data subject in their possession that is inaccurate, irrelevant, excessive or outdated.
(3) *Right to prevent processing:* A data subject must have the right to require the data controller to cease or not begin processing of personal information for a specified purpose or in a specified manner.
(4) *Right to prevent processing of personal data for direct marketing:* A data controller must not process the data subject's information for direct marketing purposes without the prior consent of the data subject.
(5) *Rights in relation to automated decision-taking:* A data subject is entitled to require the data controller to ensure that any decisions taken by or on behalf of the data controller which significantly affect him/her are not based solely on processing by automatic means.
(6) *Rights in relation to exempt manual data:* A data subject has the right to require the data controller to rectify, block, erase or destroy manual data which is inaccurate or incomplete or to cease holding such data in a manner which is incompatible with the legitimate purposes pursued by the data controller.

Cross-Border Data Sharing

When considering the cross-border sharing of data for research, all the provisions of the Data Protection Act must be met. The Act has no specific requirements on cross-border data sharing.

Therefore, a researcher who wants to transfer personal data outside Ghana must comply with the general principles and regulations in the Act.

LEGAL REGULATION OF AI

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

There is no specific legislation of AI or a particular legislative provision that addresses AI-related issues, including predictive algorithms. There is also no technological provision, industry- or sector-specific guidance. 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 specific AI strategy, but there are strategies on digital transformation and innovation, such as the National Broadband Strategy, 2018–2023. Ghana has the opportunity to develop and implement a national broadband strategy as indicated in the Information Communications Technology (ICT) for Accelerated Development and Telecom Policies, which was advanced by a coalition of stakeholders. The strategy is meant to ensure the uptake of broadband in Ghana as an economic stimulus by making it accessible and affordable, and by looking at how it would contribute to GDP growth and human development.

Digital Health/E-Health

The available strategy and policy are the National e-Health Strategy 2010 and the Ghana National Health Policy Guide on Digital Health. The E-Health Pharmacy Policy 2021 and Health Sector ICT Policy and Strategy of 2005 complement the e-Health strategy. The Health Professions Regulatory Bodies Act, The Medical Profession (Professional Conduct and Ethics) Regulations

and the Ghana Health Service Code of Conduct and Disciplinary Procedures regulate health professionals. The Ghana Public Health Act and the Guidelines for Clinical Trials, together with various institutional ethics review boards, regulate and direct medical research.

The Food and Drugs Authority established by the Public Health Act regulates medical devices in Ghana. However, no specific legislation provides for AI use in medical devices.

Consumer Protection and E-Legislation

Consumer protection	The regulatory framework for consumer protection is fragmented and includes: the Sale of Goods Act, Hire Purchase Act, Contracts Act, and Electronic Transactions Act. There are certain institutions with a general mandate in this area. These include the Ghana Standards Authority, established in terms of the Standards Authority Act, and the Food and Drugs Authority operating in terms of the Food and Drugs Act.
ICT/E-legislation	• Cybersecurity Act • Data Protection Act • Electronic Communications Act • Electronic Communications Regulations • Electronic Transactions Act • National Communications Authority Act • National Information Technology Agency Act

Data Protection Law

While no AI 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.

There are six minimum standards of data collected fairly and lawfully:

(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.

Particularly important are restrictions on the processing of sensitive (health/genomic) data and the prohibition on automated decision-making:

- The processing of special personal data is prohibited. Exceptions include instances in which the data subject has consented or where processing is necessary for: the exercise of a right or obligation imposed by law on an employer or the protection of the vital interests of the data subject where consent has not been obtained. Special personal data may be processed only for the protection of the legitimate activities of non-profit political, philosophical, religious or trade union bodies where such processing relates to individuals who are members or have regular contact with the body and it does not involve disclosure of the personal data to a third party without the consent of the data subject. Processing of special personal data is understood to be necessary where it is required for legal or medical purposes and it is undertaken by a health professional pursuant to a duty of confidentiality. Medical purposes are further defined to include preventive medicine, medical diagnosis, medical research, provision of care and treatment and management of healthcare services by a medical or dental practitioner or a legally recognised traditional healer. Personal data related to the physical or mental health of a data subject must not be disclosed unless required by law.
- A data subject is entitled to request the data controller to ensure that any decision taken is not based solely on the automated processing of data. Nonetheless, where such a decision significantly affects an individual, the data controller must inform the data subject that the decision was made on that basis as soon as reasonably practicable and the data subject may request that the decision be reconsidered within 21 days after receipt of this notice. Within

21 days, the data controller is subsequently required to inform the data subject of the steps they intend to take to comply with the notice. Where the Commission is satisfied that the data controller has failed to comply, they may order them to do so. Such a compliance order will not affect individuals other than the data subject or data controller.

Intellectual Property

Copyright Act

The permitted use of work protected by Copyright in the Ghana Copyright Act is inadequate, and is a dilemma for librarians. The reproduction of a book is limited to sections or chapters of a book, even though students need unlimited access to complete books. Libraries that are not for gain are restricted to making only a single copy of a book for replacement or for preservation. This will aggravate the chronic shortage of books and materials for students. Of note is that the Berne Convention does not expressly restrict the number of copies of material that can be made for teaching purposes. It is therefore unnecessary to restrict the number of copies that can be made under the permitted use clause. Libraries and archives could be allowed to make a reasonable number of copies of highly used but otherwise unavailable books for research and preservation, with limited impact on the author, given that students have access to a book and after they have read it they may want to buy it. In addition, the permitted use clause is limited to libraries and archives with activities that are not for gain. This is unfair to private tertiary institutions and universities that have large numbers of students. Libraries and librarians are, unfortunately, portrayed as enforcers and controllers of copyright rather than as service providers.

Patents Act

The Patents Act and the Patents Regulations are the legislative framework for the granting and protecting of patents in Ghana. The Patents Office of the Registrar General's Department is the issuing office of patents. Patents are territorial and therefore the grant of a patent in Ghana affords the inventor the rights and protection of the invention only within Ghana. A patent may also be granted in respect of Ghana by filing a regional patent application with the African Regional Industrial Property Organisation (ARIPO). The World Intellectual Property Organization (WIPO) administers the Patent Corporation Treaty (PCT).

The Patents Act excludes some inventions from the granting of patents. These include: (i) discoveries, scientific theories and mathematical methods; (ii) methods for conducting business or playing purely mental games; and (iii) inventions contrary to public policy and morality. The legislative framework also makes provision for the granting of rights and protection over inventions that do not qualify for patent protection. In such an instance, a utility model certificate may be granted in respect of new and industrially applicable inventions under the Patents Act.

The Patents Act provides that the right to a patent belongs to the inventor, but it is not clear that such a provision can be expansively interpreted to accommodate the AI system. Definitions of applicants or inventors in the Copyright and Patent Acts do not treat AI systems as being lawfully recognised as inventors.

Summary and Analysis

Ghana has produced strategy/policy documents aimed at digital transformation, but these do not directly address AI regulation. While a number of policy documents guide digital heath implementation, no specific legislation provides for AI use in medical devices. The above policy documents are interoperable and do not supersede one another; however, relevant provisions in legislation will take precedence over other regulatory/policy documents.

The Data Protection Act restricts the processing of personal data and its prohibition on automated decision-making is vital in the regulation of AI systems. Ghana's framework for consumer protection is fragmented and there is no consumer protection legislation. Accordingly, little protection for AI technologies may be found. Regardless, ICT/E-legislation and a consideration of intellectual property legislation, jurisprudence and soft law may be essential in ensuring that these technologies are used properly.