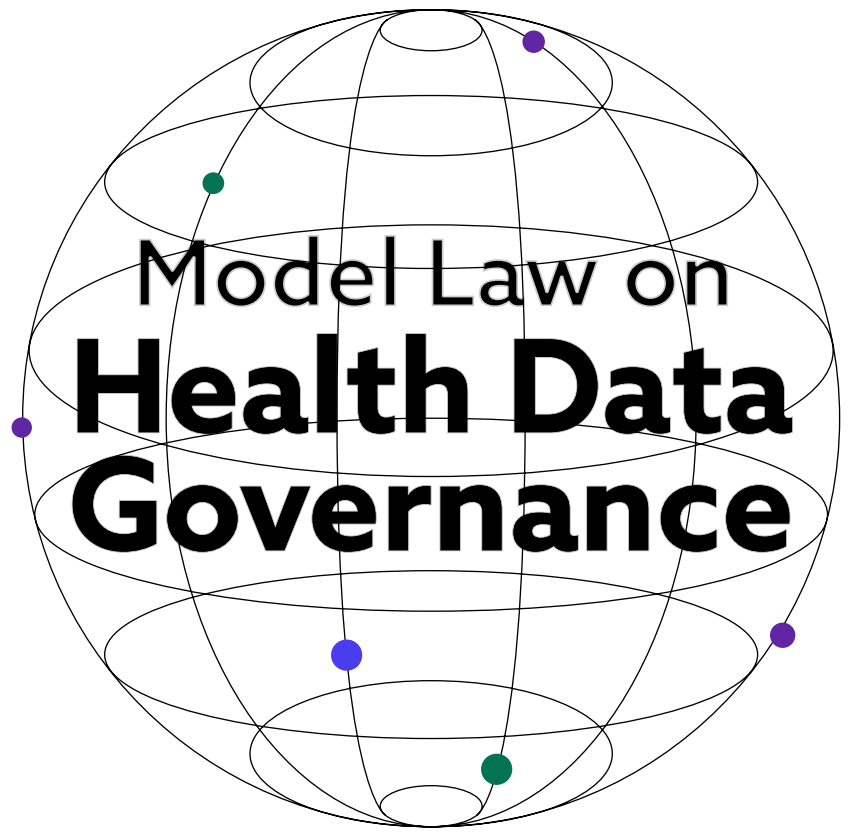


Model Law on **Health Data Governance**

Public Consultation Draft

PUBLIC CONSULTATION PERIOD 7TH APRIL - 30TH APRIL 2024



Responsible Entity: Transform Health

Drafted by: Dr Marietjie Botes, Paul Esselaar, Prof Donrich Thaldar

Version issued: 6 April 2024

PREFACE

As the generation of digital health data grows exponentially, this requires the safeguarding of individual and community rights while fostering an environment of trust, innovation, and equitable access. The advent of sophisticated technologies has transformed the landscape of health data management and use, necessitating a legal framework that is both resilient and adaptable to the ever-evolving digital health ecosystem

Aim of this model law

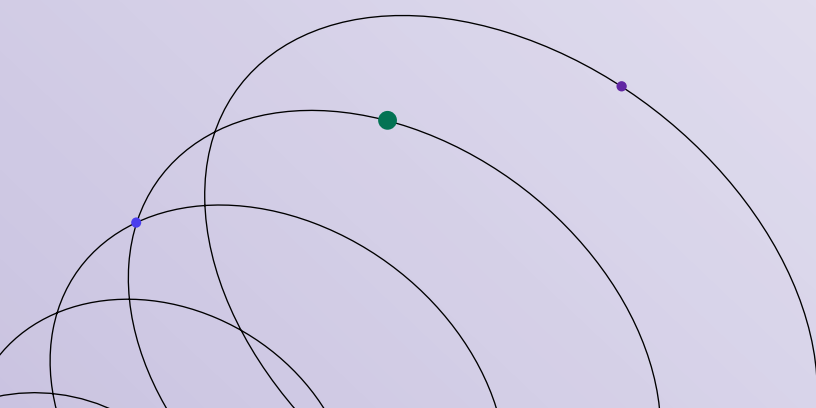
This model law aims to strike a delicate **balance between the protection of personal and community health data** and the facilitation of its **use for the greater public benefit**, ensuring that progress in health data use is anchored in principles of equity, justice, and respect for human rights. By establishing clear rights, responsibilities, and safeguards, this model law aspires to foster an environment where **health data can be used as a force for good**, driving improvements in healthcare, research, and public health policies. It also addresses the challenges and opportunities presented by emerging technologies, ensuring that innovation in health data use does not come at the expense of fundamental human rights.

Although this Model Law is intended to create a framework for health data governance, it will require the publication of subsidiary legislation to provide further detail—tailored for a specific country's culture and context. In addition, a regulatory body may be required to manage health data governance across different legal instruments.

Providing legislative guidance and reference text (non-prescriptive)

The primary intention of this model law is to **offer guidance to countries aiming to integrate its principles and standards (or relevant sections of it) into their existing national legislation or develop new laws where and if needed. It is designed to be non-prescriptive and allows for flexibility and adaptability to local contexts and needs.** It serves as legislative guidance and sample reference text to assist countries with their efforts to strengthen their national laws and frameworks dealing with health data governance. Different parts of the Model Law can be inserted into different existing laws or implemented as a single health data governance law, depending on the national context.

The law provides a foundational structure for the ethical management, protection, and use of health data, emphasising the balance between individual privacy rights and the collective benefits of health data utilisation. By setting out core principles and standards, it seeks to foster a harmonised approach to health data governance that respects the diverse legal, cultural, and societal landscapes of different nations.



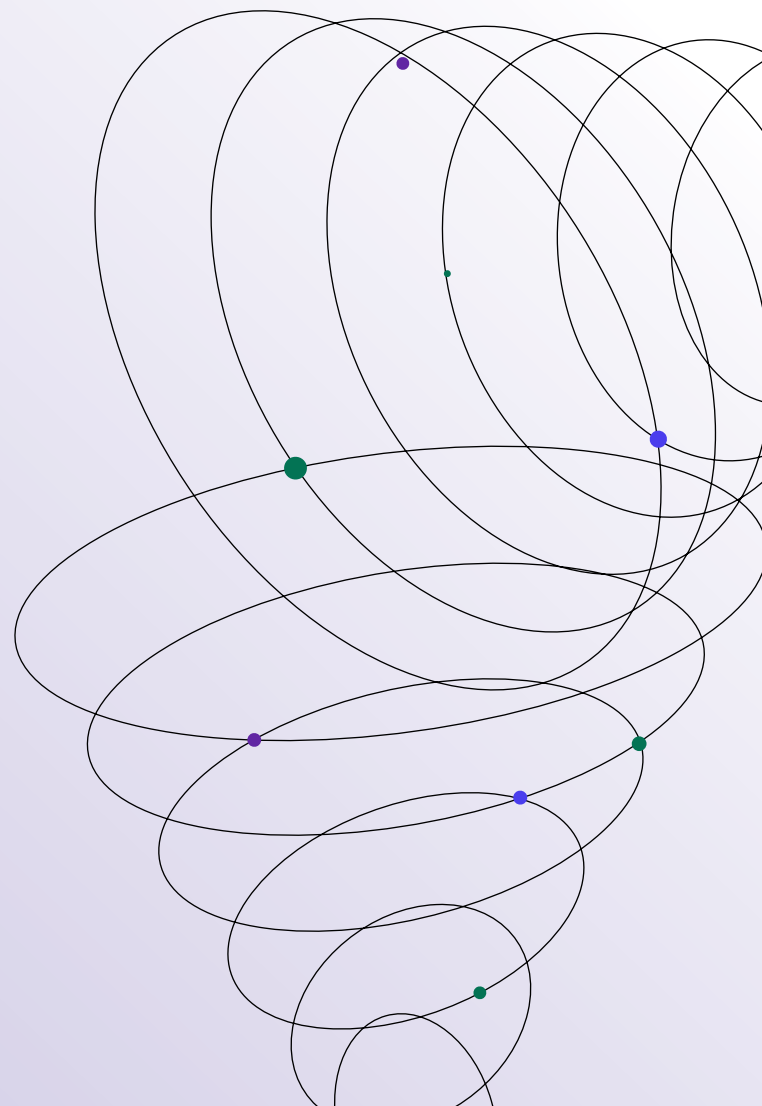
Advantages of a model law

While principles provide broad guidance, a model law lays out specific legal provisions, definitions, and mechanisms that can be directly incorporated or customised to fit within existing national laws. **A model law can more effectively address complex issues related to data rights, privacy, and consent**, providing clear legal pathways for enforcement and compliance. This leads to stronger protection for individuals and communities and a more robust legal foundation for managing health data ethically and responsibly.

The Model Law provides the **foundation for a global health data governance framework, the endorsement of which by governments through a World Health Assembly (WHA) resolution**, would build consensus across countries around the core principles and standards that should be addressed through national legislation and regulation for the effective and equitable governance of health data. This provides a process for Member States to discuss, evaluate, and ultimately adopt this model law. While a WHA resolution itself does not have direct legislative authority over individual countries, it can influence global health policy and establish consensus across countries. The practical impact of the endorsement of a WHA resolution for individual countries would include standardised health data governance practices, the provision of guidance and best practices for countries to follow when developing their own health data governance frameworks, the facilitation of interoperability between health systems and data sharing across borders, the protection of individual and communal rights, and greater collaboration among countries in sharing data for research, surveillance, and public health interventions, while reducing ambiguity and variation in interpretation that can arise from principles alone.

Data Protection law must exist

This model law operates on the assumption that **countries already possess an existing data protection law or data protection regulatory framework** to ensure that it complements and enhances the current legal structures, rather than conflicting with them or duplicating efforts. Cognisant of the fact that the maturity of digital health infrastructure and regulatory frameworks may differ between countries, this model law also tries to address variations in this regard. It acknowledges the groundwork laid by these frameworks in establishing fundamental data protection principles and aims to build upon this foundation with specialised attention to health data's unique aspects and challenges.



Choice of a Model Law as an instrument

In comparison with related regulatory instruments such as guidelines, policies, or even checklists, a model law was the preferable convention for the procurement of goods, construction, and services,¹ and the regulation of international e-commerce.² For example, in 1993/1994 the UNCITRAL Model Law on Procurement of Goods, Construction and Services which provides a template for reforming regulatory systems on public procurement was adopted. In 2004, this template was reviewed for updates to keep track with changes in the latest purchasing practices, electronic procurement, and the increasing need for harmonisation with other international norms. Similarly, in the context of health data governance, the advantages of using a model law “template” over any other regulatory instrument include the following:

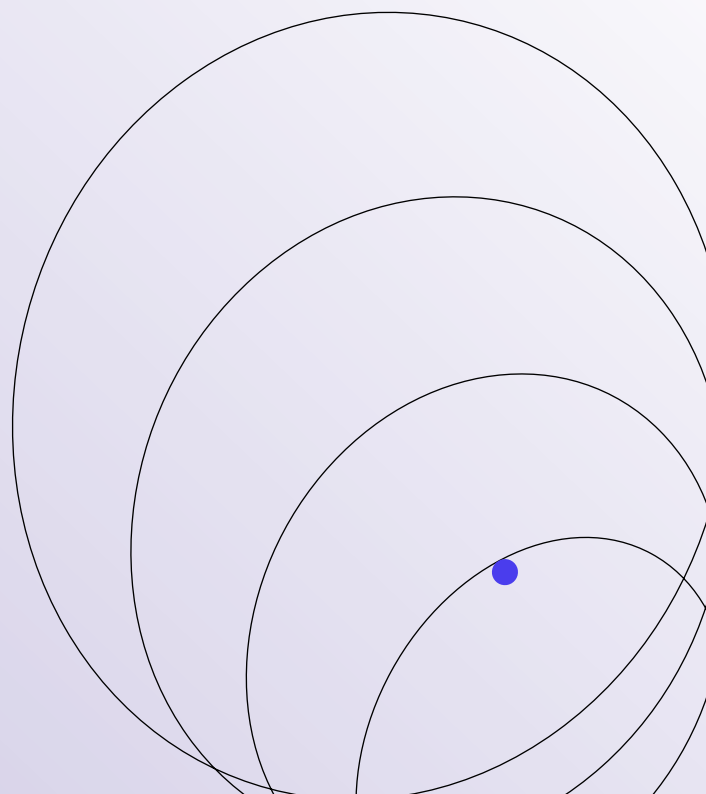
- **Flexibility:** Model laws are designed to provide a flexible framework that can be adapted to suit the legal systems of different countries. This flexibility allows jurisdictions to tailor the law to their specific needs while still maintaining consistency with international standards.
- **Harmonisation:** Model laws facilitate the harmonisation of laws across different jurisdictions. By providing a common framework, model laws help to reduce legal inconsistencies and barriers to international health data sharing.

- **Efficiency:** Model laws can streamline the legislative process by providing a ready-made template for lawmakers to use. This can save time and resources compared to drafting new legislation from scratch.
- **International Cooperation:** Model laws promote international cooperation by providing a basis for countries to work together in developing common legal standards. This cooperation is essential for addressing global issues such as e-commerce and health data governance, where cross-border transactions and data sharing are common.
- **Legal Certainty:** By adopting a model law, countries can benefit from greater legal certainty in their health data governance. This can help to build trust among individuals, communities, health data generators, and health data holders, leading to increased confidence in the health data governance space.

Overall, a model law offers a pragmatic and effective approach to regulating complex areas such as health data governance, providing a balance between harmonisation and flexibility that can accommodate the diverse legal systems and interests of different countries.

1 Arrowsmith S. Public Procurement: An Appraisal of the Uncitral Model Law as a Global Standard. *International and Comparative Law Quarterly*. 2004;53(1):17-46. doi:10.1093/iclq/53.1.17

2 Haines AD. Why is it so difficult to construct an international legal framework for e-commerce? *The Draft Hague Convention on Jurisdiction and the Recognition and Enforcement of Foreign Judgments in Civil and Commercial Matters: A Case Study*. *European Business Organization Law Review*. 2002;3(1):157-194. doi:10.1017/S1566752900000859



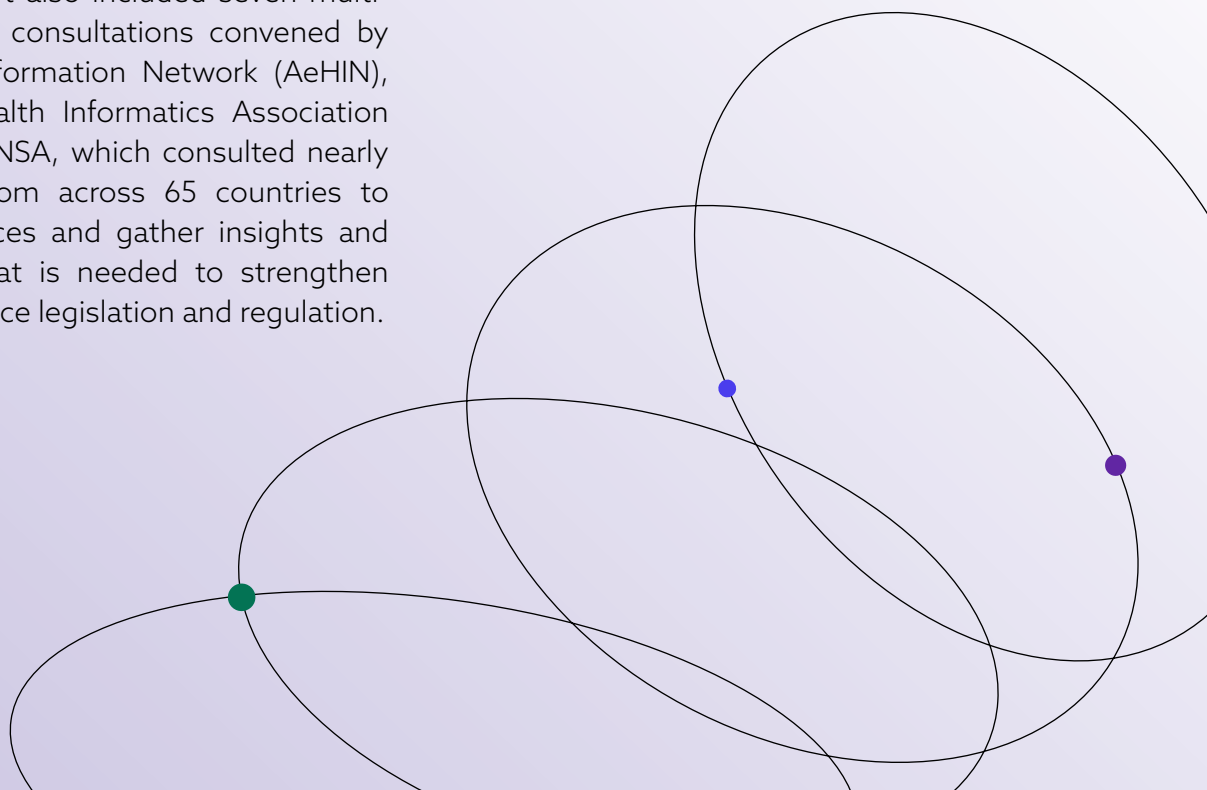
Development of the Model Law

This draft Model Law has been informed by [equity and rights-based health data governance principles](#), the [OECD Recommendation on Health Data Governance](#), [European Union General Data Protection Regulation \(GDPR\)](#), the [Health Insurance Portability and Accountability Act \(HIPAA\)](#), [standards issued by the International Organization for Standardization \(ISO\) 27799](#), the [Council of Europe's Convention 108](#), the World Health Organizations' (WHO) Guidelines on Data Privacy and Protection in Health Information Systems, the [International Ethical Guidelines for Health-related Research Involving Humans \(CIOMS Guidelines\)](#), the [OECD Privacy Guidelines and Recommendations of Health data Governance](#), the [International Conference of Data Protection and Privacy Commissioners \(ICDPPC\) Resolutions](#), the [United Nations Convention on the Rights of Persons with Disabilities \(CRPD\)](#), and the [Health Data Charter by the Global Partnership for Sustainable Development Data](#), among other national, regional and international commitments and best practice. It has also been informed by national legislative and regulatory landscape reviews of more than 30 countries, as well as a review of relevant literature, strategies, reports, and instruments. The process to inform the consultation draft also included seven multi-stakeholder regional consultations convened by the Asia eHealth Information Network (AeHIN), the Pan African Health Informatics Association (HELINA) and RECAINSA, which consulted nearly 500 stakeholders from across 65 countries to learn from experiences and gather insights and perspectives on what is needed to strengthen health data governance legislation and regulation.

Consultation process

This consultation draft of this Model Law has been shaped by inputs from the Africa CDC Flagship Initiative on Health Data Governance working group and the Transform Health Policy Circle and Health Data Governance working group. An advisory group was set up to provide expert guidance and feedback on the draft, which includes representatives from ETH Zürich (Health Ethics and Policy Lab, Institut für Politikwissenschaft (Department of Political Science), Instituto De Efectividad Clínica Y Sanitaria (IECS), OECD, Palladium Group, PharmAccess, Resolve to Save Lives, Transform Health, University of Copenhagen (Department of Public Health), University of St. Gallen (HSG), and World Health Organization (WHO).

A public consultation period on the draft Model Law was convened between the 7th and 30th of April 2024 with the aim of gathering wide stakeholder and expert feedback to strengthen the draft, and building consensus, alignment and support. The consultations period included [add details], which saw inputs from [add] stakeholders from across [add] countries/constituencies. [further details from the public consultation period to be added].



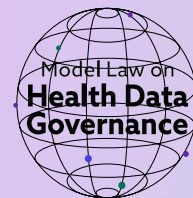


TABLE OF CONTENTS

1. PURPOSE	6
2. DEFINITIONS	7
3. SCOPE	8
4. EXCLUSIONS	8
5. INTERPRETATION	8
6. HEALTH DATA EQUITY TRIBUNAL	9
7. PORTABILITY OF ELECTRONIC MEDICAL RECORDS	10
8. COMMUNITIES' RIGHTS IN THEIR COMMUNITY HEALTH DATA	11
9. RIGHTS AND OBLIGATIONS OF HEALTH DATA GENERATORS	12
10. PROHIBITION ON RE-IDENTIFICATION	12
11. USING HEALTH DATA IN THE PUBLIC INTEREST	13
12. HEALTH PANDEMICS AND OTHER HEALTH EMERGENCIES	14
13. EMERGING TECHNOLOGIES	15
14. FEEDBACK, CONFIDENTIALITY, AND PROTECTION OF WHISTLE-BLOWERS	16
15. RESOLUTION OF DISPUTES AND THE RIGHT OF REDRESS	16
16. OFFENCES	17
17. PENALTIES	18
18. SUBSIDIARY LEGISLATION	18
19. REVIEW	19
20. TRANSITIONAL PROVISIONS	19
21. SHORT TITLE AND COMMENCEMENT	19
APPENDIX A: AMENDMENTS TO DATA PROTECTION LEGISLATION	20

1. PURPOSE

This Law seeks to augment the existing [Data Protection Law] to create a balanced and effective legal framework for health data governance that respects and protects individual privacy and rights while enabling the beneficial use of health data for societal benefit such as research, innovation, policymaking, patient safety, personalised medicine, official statistics or regulatory activities. In addition, the goal is to improve the functioning of global health data governance by laying down a uniform legal framework in particular for the development, marketing, and use of health data in conformity with global standards and principles. More specifically this model law seeks to:

- a. Protect the proprietary interests in health data:** Ensure that the proprietary rights in health data of persons that collect and generate health data are recognized and protected, as to create a conducive environment for research and innovation.
- b. Ensure the Protection of Health Data:** Establish comprehensive and robust protections and guarantees for personal health data, ensuring the privacy, integrity, and security of such data against unauthorised access, use, disclosure, alteration, and destruction.
- c. Promote Transparency and Accountability:** Require transparency in the collection, use, access, storage, sharing and disposal of health data, and hold individuals, communities, data controllers and health data generators involved in the processing and management of health data accountable for compliance with this Act.
- d. Facilitate Ethical Use of Health Data:** Promote the ethical collection, analysis, and use, access, storage, and disposal of health data for healthcare planning and delivery, disease surveillance, public health, research, and innovation, ensuring that such activities are conducted with respect for individual and communal rights and are in the public interest.
- e. Enhance Public and Individual Health Outcomes:** Leverage health data to improve public health policies, improve the effectiveness and efficiency of health planning and budgeting, improve healthcare quality, and efficiency, while ensuring that the benefits of health data use are distributed fairly across society.
- f. Support Health Research and Innovation:** Foster an environment that supports health research and innovation, by providing clear rules for the ethical use of health data in research, development of medical technologies, and other related scientific endeavours.
- g. Safeguard Individual and Community Rights:** Ensure the protection of individuals and communities' rights in relation to their health data, including the right to access, correct, and control the use of their personal health information.
- h. Promote Data Literacy:** Encourage the development of health data awareness and literacy among the public and stakeholders.
- i. Establish Governance and Oversight Mechanisms:** Create effective governance structures and oversight mechanisms to ensure that health data is managed in accordance with the duties and obligations set forth in this act, and to address any violations or challenges that arise.
- j. Adapt to Technological Advancements:** Provide a flexible and adaptive legal framework that can accommodate future technological advancements in health data collection, analysis, and use, ensuring that the law remains relevant and effective in a rapidly evolving digital landscape.

2. DEFINITIONS

In this Law, unless the context clearly indicates otherwise, the following terms have the corresponding meanings:

- a. **"Anonymisation"** means the process of irreversibly transforming personal data into a form in which the individual to whom the data relates cannot be identified, directly or indirectly, while still allowing the data to be used for legitimate purposes.
- b. **"Community"** means a group of natural persons who share a common geographic location, heritage, culture, or social identity, and who collectively contribute to health data and includes but is not limited to indigenous communities, patient groups with specific health conditions, and populations within a defined geographical area;
- c. **"Community health data"** means health data that contain information that is significant to the identity, heritage, cultural practices, or collective health of a community as a whole;
- d. **"Controller"** means the person responsible for determining the purposes and means of the processing of health data;
- e. **"Electronic medical record"** means a digital collection of a patient's medical history, treatments, diagnoses, laboratory testing results, immunizations, and other health-related information maintained and held by a healthcare provider;
- f. **"Healthcare provider"** means any person offering health services, including health professionals, as regulated by [relevant legislation that regulates health professionals], and any facility, like hospitals, clinics, and other institutions, that provide health services, like treatments and diagnostics, whether they operate for profit or not;
- g. **"Health data"** means data related to human health, irrespective of whether such data can identify such person or not and includes personal-level data, population-level data, facility data, and system data that relate to human health;
- h. **"Health data generator"** means a person who collects or generates health data and stores such health data in a digital format;
- i. **"Personal health data"** means health data that relate to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- j. **"Processing"** means any operation, activity, or any set of operations, whether or not by automatic means, concerning health data;
- k. **"Pseudonymisation"** means the processing of personal health data in such a manner that the personal health data can no longer be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal health data are not attributed to an identified or identifiable natural person;
- l. **"Re-identification"** means the process by which information is attributed to de-identified data in order to identify the individual to whom the de-identified data relate;
- m. **"Regulator"** means the body responsible for the regulation of the [data protection law];
- n. **"Tribunal"** means the Health Data Equity Tribunal as created by this Act in section 6;

3. SCOPE

1. This Law applies to all persons, whether natural or juristic, involved in the collection, generation, processing, storage, use, access, sharing and disposal of health data within [Country/Jurisdiction]. This includes, but is not limited to, healthcare providers, health insurance companies, health information technology companies, research health data holders, and any other organisations processing or managing health data.
2. This Law covers health and health related data relating to the physical or mental health of an

individual or community, including medical histories, diagnoses, treatment information, genetic data, and other data deemed sensitive under this act. This encompasses both digital and non-digital formats of health data.

3. This Law applies to the processing of health data within [Country/Jurisdiction], including the processing of such data by health data holders located outside [Country/Jurisdiction] if the data pertains to individuals and/or communities within [Country/Jurisdiction].

4. EXCLUSIONS

This Act does not apply to:

- a. Health data collected, processed, stored, or used for personal or household activities with no connection to a public or professional context;
- b. Personal data which is not health data;
- c. Health data which is required by a public body which are aimed at assisting in the identification and financing of terrorist and related activities, money laundering, defence or public safety;
- d. Journalistic, literary or artistic expression, provided that the Tribunal or a court is empowered to determine whether the right to freedom of expression prevails over the rights of individuals or communities in their health data as set out in this Act;
- e. The judicial functions of a court.

5. INTERPRETATION

The use in this Law of possessive pronouns with relation to health data is intended to indicate that such health data relates and identifies the relevant individual or community; it should not be interpreted as indicating legal possession or ownership.



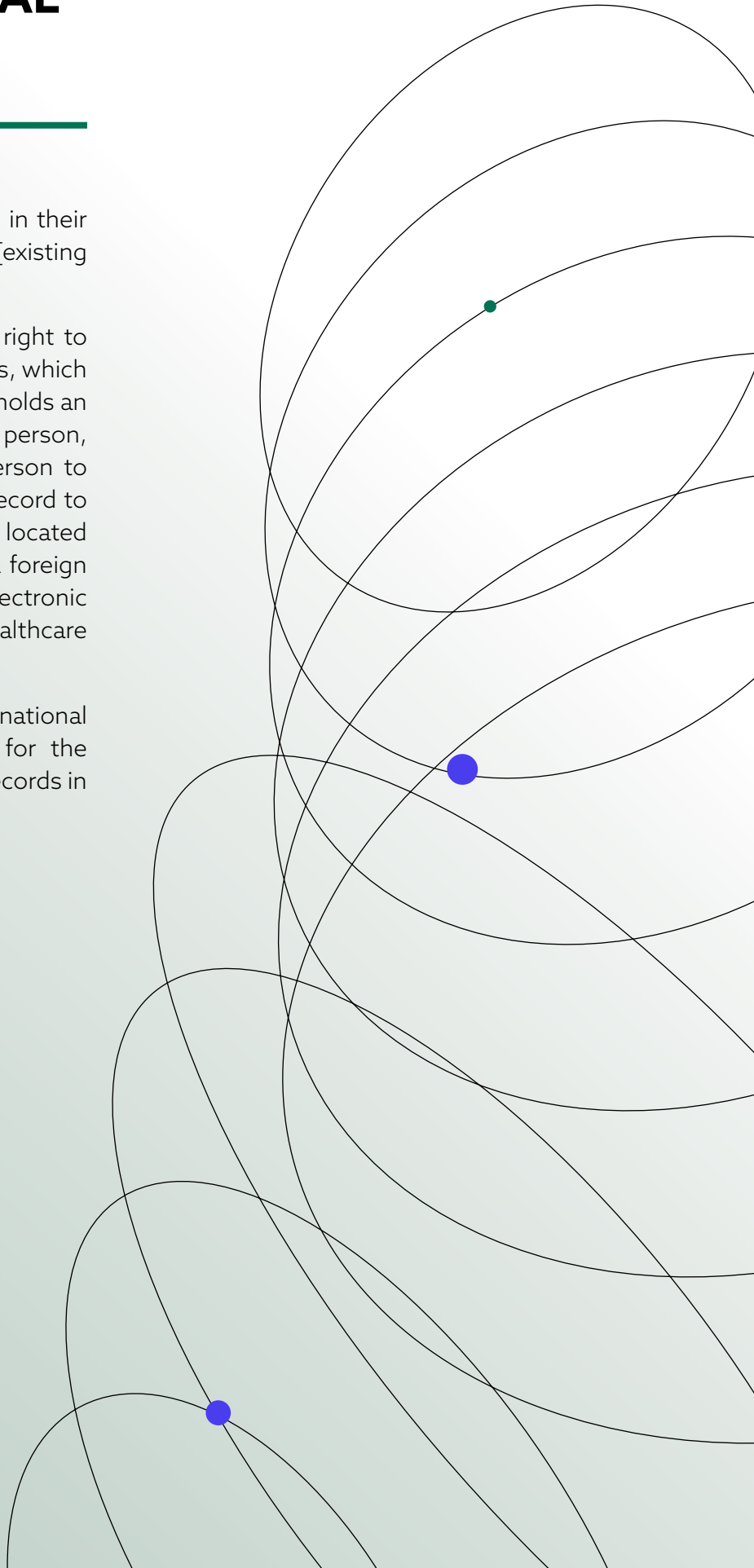


6. HEALTH DATA EQUITY TRIBUNAL

1. This Act establishes the Health Data Equity Tribunal (the "Tribunal") to adjudicate matters related to the governance, use, and protection of health data within [Country/Jurisdiction].
2. The objective of the Tribunal is to ensure the fair, transparent, and efficient resolution of disputes arising under the [Model Law on Health Data Governance] and to provide oversight on matters related to the ethical use, privacy, and security of health data.
3. The Tribunal shall have jurisdiction over all matters arising under the [Model Law on Health Data Governance], including disputes between the Regulator, individuals, communities, health data holders and health data owners and the imposition of penalties for violations.
4. The Tribunal is empowered to hear cases, make determinations, order remedial actions, impose penalties, and take any other actions deemed necessary to enforce the provisions of the [Model Law on Health Data Governance].
5. The Tribunal shall consist of [a specified number] of members, including a Chairperson, with expertise in health data management, law, ethics, and technology.
6. Members of the Tribunal shall be appointed by [the appointing authority] for a term of [number] years, renewable once. Selection shall be based on demonstrated expertise and integrity.
7. The Tribunal shall establish its own procedures for the hearing of cases, in accordance with principles of natural justice and fairness. Proceedings may be conducted in person, in writing, or electronically, as appropriate.
8. Decisions of the Tribunal can be appealed to [the higher court or body] within [number] days of the decision, on matters of law or jurisdictional error.
9. All decisions of the Tribunal are binding and enforceable. Failure to comply with a decision of the Tribunal constitutes an offence under the [Model Law on Health Data Governance].
10. The Tribunal shall publish annual reports on its activities, decisions, and the state of health data governance within [Country/Jurisdiction], while respecting confidentiality and privacy obligations.
11. The Tribunal shall be funded by [source of funding], and shall have access to the necessary resources, staff, and facilities to effectively carry out its functions.
12. Health data holders, communities, individuals, and health data owners have the right to appeal against decisions made by regulatory authorities regarding the determination of offenses and the imposition of penalties, through judicial review or other legal mechanisms provided by law.
13. In addition to penalties, offenders may be required to provide restitution to affected data subjects, compensating them for any harm caused by the offense.
14. The Tribunal may also order remedies, including the implementation of specific measures to rectify violations and prevent their recurrence.
15. In determining penalties, consideration shall be given to aggravating factors, such as the scale of the offense, the sensitivity of the data involved, and the vulnerability of affected data subjects and mitigating factors, such as voluntary reporting of offenses, cooperation with investigations, and measures taken to prevent future offenses, may be considered to reduce the amount of damages awarded to the claimants.

7. PORTABILITY OF ELECTRONIC MEDICAL RECORDS

1. All natural persons have privacy rights in their personal health data as provided for in [existing data protection legislation].
2. In addition, natural persons have the right to portability of electronic medical records, which means that a healthcare provider that holds an electronic medical record of a natural person, shall, upon request by the natural person to transfer his or her electronic medical record to another specified healthcare provider, located either in [Country/Jurisdiction] or in a foreign country, transfer a copy of such electronic medical record to the specified healthcare provider without delay.
3. The Regulator, having regard to international standards, shall establish standards for the interoperability of electronic medical records in guidelines.



8. COMMUNITIES' RIGHTS IN THEIR COMMUNITY HEALTH DATA

1. A community shall act through its representative body for purposes of this Act.
2. The [relevant national authority] shall establish transparent mechanisms in subsidiary legislation regarding:
 - a. the criteria for a person or persons to be recognised as the representative body of a community for purposes of this Act, and
 - b. for supporting the effective functioning of representative bodies.
3. A controller may only process a community's community health data if such community agreed to such processing.
4. A community may provide consent subject to any conditions, including that it will receive specified benefits: provided that such conditions do not contravene any other legal norm.
5. The [relevant national authority] shall establish guidelines for appropriate conditions as contemplated in subsection (4).
6. Consent by a community to the processing of its community's health data does not replace or detract in any way from the rights of individual members of the community in terms of [existing data protection legislation].
7. Any member of a community who disagrees with the decision of such community's representative body with regard to the processing of the community's community health data, has the right to petition the representative body to change its position, and if the disagreement is not resolved following the petition, to apply to the Tribunal to review the decision of the representative body in terms of [existing administrative law legislation / the common law principles of administrative justice].
8. A controller must secure the integrity and confidentiality of community health data in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent:
 - a. loss of, damage to, or unauthorised destruction of community health data; and
 - b. unlawful access to or processing of community health data.



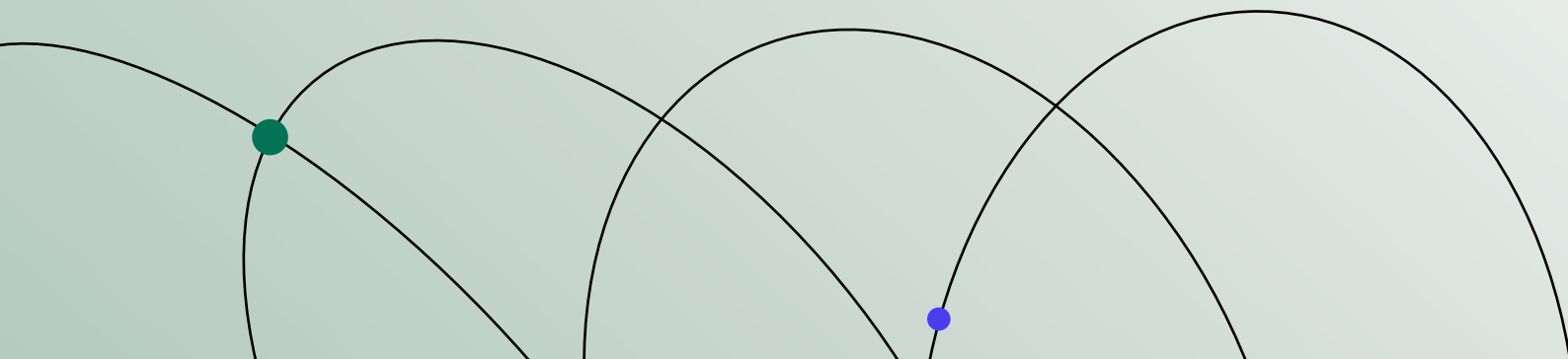
9. RIGHTS AND OBLIGATIONS OF HEALTH DATA GENERATORS

By virtue of collecting or generating health data and storing such health data in digital format, a health data generator obtains proprietary rights in the digital instances containing such health data, which rights are freely transferable, provided that:

- a. If such proprietary rights are in conflict with a natural person's privacy rights as contemplated in section 7, the natural person's privacy rights will supersede such proprietary rights to the extent of the conflict.
- b. The same applies mutatis mutandis if such proprietary rights are in conflict with a community's rights as provided in section 8.
- c. Where a person who holds any proprietary rights as contemplated in this subsection have duties in terms of [existing data protection legislation], such person shall enforce such proprietary rights to fulfil such duties.

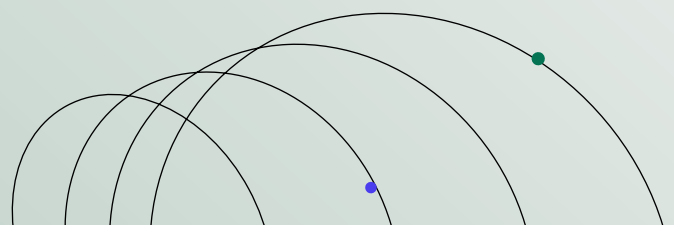
10. PROHIBITION ON RE-IDENTIFICATION

1. No person who obtains, possesses, or has access to anonymised or pseudonymised personal health data shall intentionally engage in any action with the purpose or effect of re-identifying the said data.
2. This prohibition shall not apply to persons authorised by the health data generator or Tribunal for the sole purpose of testing the robustness of anonymisation or pseudonymisation processes.
3. Any person who, in the course of their legitimate activities, discovers a vulnerability that may allow for the re-identification of anonymised or pseudonymised personal health data shall report such vulnerability to the health data generator and the Regulator within [specified timeframe].
4. Upon receiving information regarding potential re-identification risks, the health data generator shall assess the risks, implement appropriate safeguards, and, if necessary, conduct a re-assessment of the anonymisation or pseudonymisation processes to strengthen data protection measures.

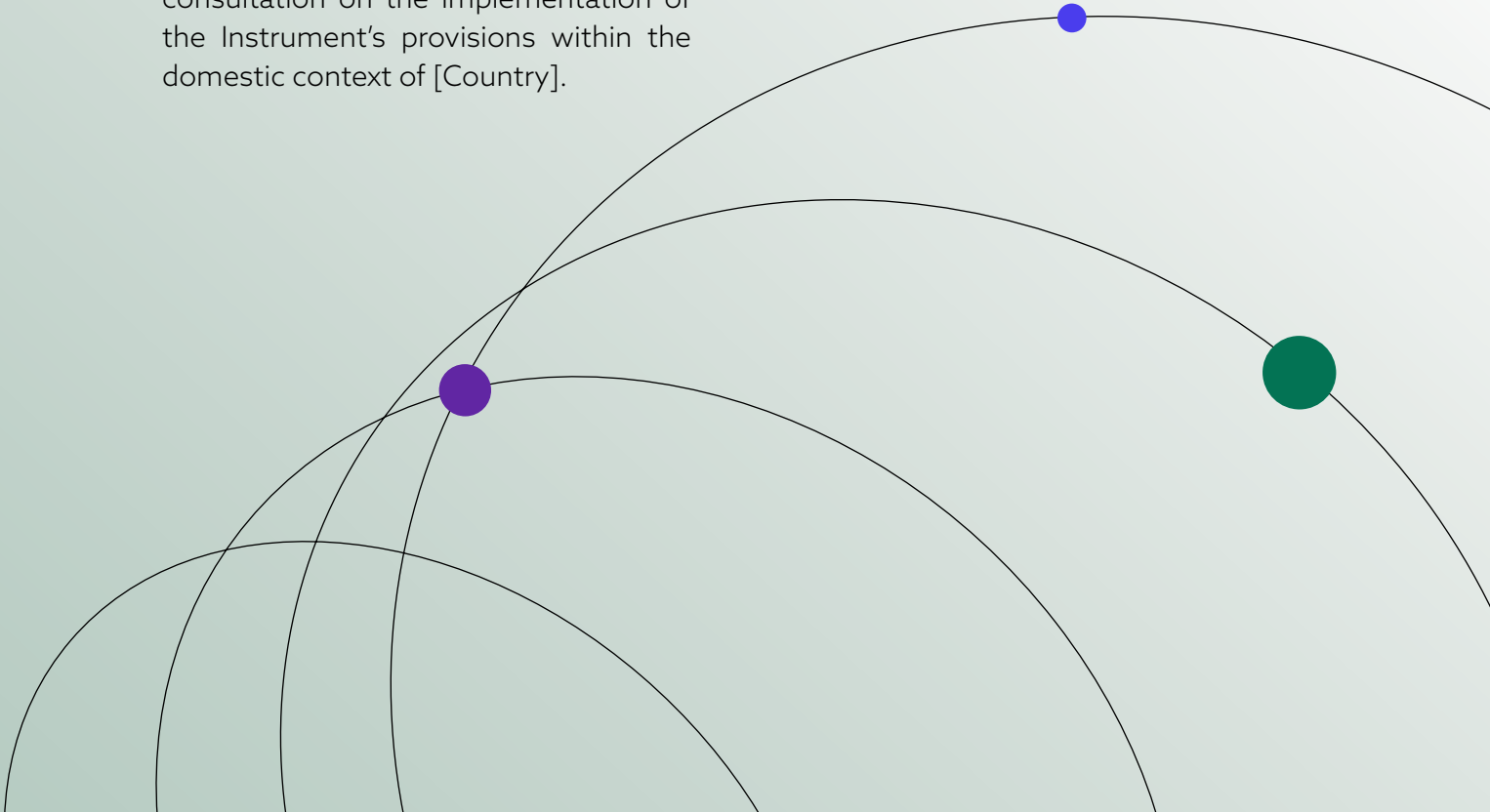


11. USING HEALTH DATA IN THE PUBLIC INTEREST

1. Any person shall, upon request by any other person, disclose whether it has any proprietary rights related to health data.
2. The [relevant national authority] may through subsidiary legislation exclude any class of juristic or natural persons from the operation of subsection (1).
3. A person who has proprietary rights related to health data shall, upon request by any other person, provide a description of the kinds of such health data in sufficient detail to enable the person making the inquiry to identify the health data that may be relevant to a potential application for a public interest use-licence under the provisions of this section.
4. Any person, hereinafter referred to as 'the applicant', may apply to the Tribunal for an order granting a use-licence for a purpose deemed to be in the public interest in specific health data that are contained in proprietary digital instances, provided that the applicant can prove that:
 - a. the intended use of such health data is for a purpose that advances the public interest, including but not limited to, public or private health research; and
 - b. the applicant has requested access to such health data from the proprietor of the digital instances containing such health data and that the request has either been refused, granted but subject to conditions that are so unreasonable that it amounts to an effective refusal, or not responded to within a reasonable timeframe.
5. In determining whether to grant a use-licence in terms of this section, the Tribunal shall consider the nature and scope of the proposed use of the health data, the potential benefits to the public, the reasons provided by the health data generator for refusing access, common practice in the relevant market, and any potential harm or risks to the natural persons and communities.
6. The Tribunal may determine a reasonable licence fee to be paid by the applicant to the health data generator for the use of the health data. The determination of the licence fee shall consider the nature of the public interest being served, the cost to the proprietor of obtaining and maintaining the health data instances, the financial position of the applicant, and any other factors the Tribunal deems relevant.
7. The Tribunal has the discretion to set the licence fee at zero if it finds that:
 - a. the use of the health data serves a paramount public interest that outweighs the commercial interests of the proprietor, or
 - b. the obtaining and/or maintaining of the health data instances was paid for to a significant extent with public funds.
8. The Tribunal shall specify the duration for which the use-licence is granted and may impose limitations on the scope of use of the health data to ensure that the use is strictly for the purpose deemed to be in the public interest.
9. The Tribunal may establish mechanisms for monitoring the use of the health data under the granted licence, to ensure compliance with the terms of the licence and the ongoing protection of individuals and communities rights and interests.

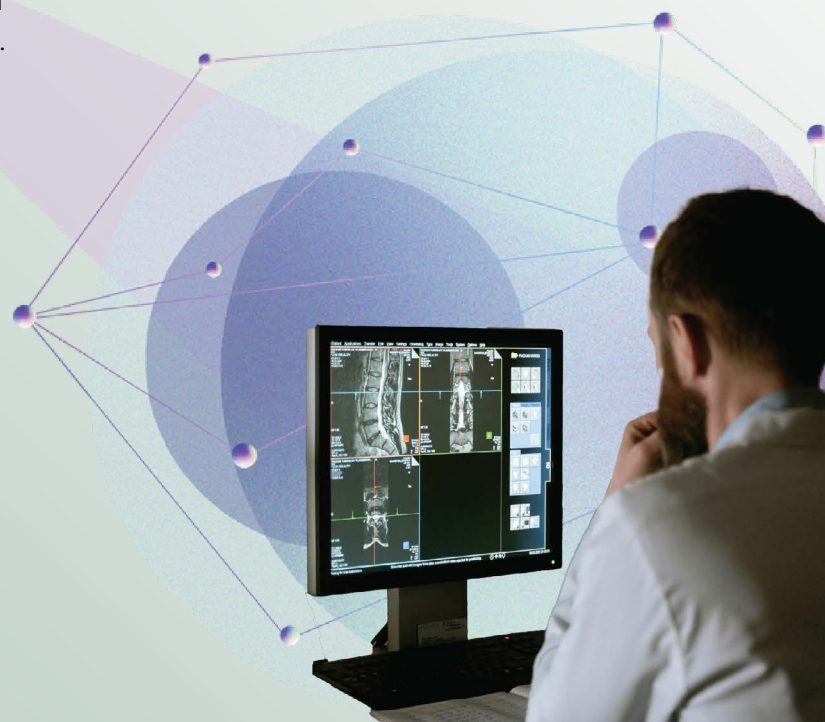


12. HEALTH PANDEMICS AND OTHER HEALTH EMERGENCIES

1. Upon ratification by [Country] of the Pandemic Prevention, Preparedness and Response Instrument, as drafted and negotiated through the intergovernmental negotiating body, for endorsement by Member States at the Seventy-seventh World Health Assembly, in May 2024,, the provisions contained within the Instrument shall be deemed incorporated in the domestic law of [Country] and shall enter into force on a date promulgated by the [member of the national executive] in the [official government notice].
 - a. the [specified national authority] shall engage in a period of public consultation on the implementation of the Instrument's provisions within the domestic context of [Country].
 - b. the [relevant national authorities] shall undertake a comprehensive review of existing legislation and policies to identify and rectify any conflicts or inconsistencies with the Instrument. The findings and recommendations from this review shall be submitted to the [national legislature] for any required amendments.
 2. Prior to the promulgation of the effective date:
 3. Following the promulgation of the effective date, and to the extent that the Accord applies to health data, the Regulator shall be empowered to issue directives and guidelines for the effective implementation of the Accord's provisions.
- 

13. EMERGING TECHNOLOGIES

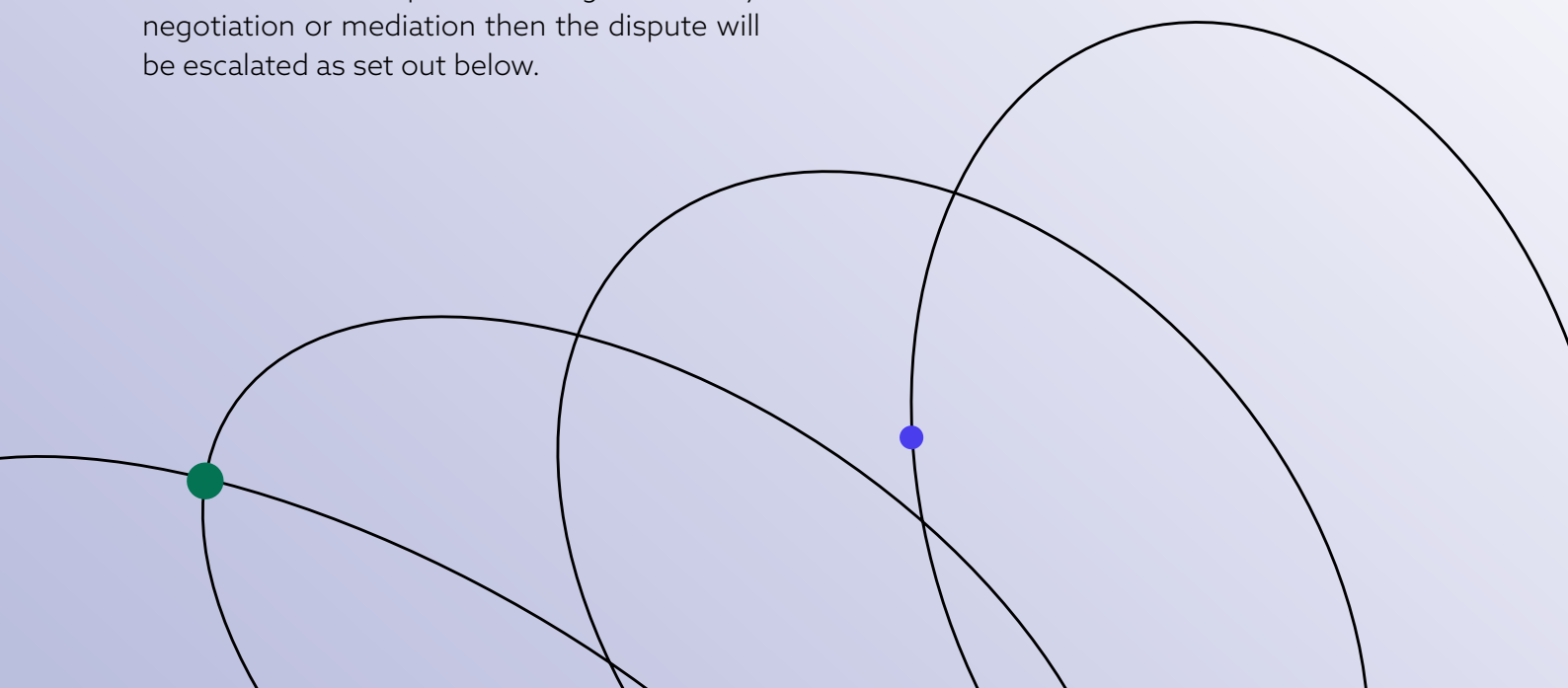
1. Individuals and communities must be provided with clear and understandable information regarding the collection, processing, and use of their health data in emerging technologies such as Artificial Intelligence (AI) and Machine Learning (ML) models, which information must allow such individuals or communities to provide informed consent as described in section 8 above.
2. All Artificial Intelligence (AI) and Machine Learning (ML) models used in healthcare settings must:
 - a. adhere to standards of transparency, ensuring that the underlying algorithms are comprehensible and interpretable by relevant stakeholders, including limitations, biases and uncertainties associated with the AI/ML models to enable informed decision making and risk assessment;
 - b. undergo rigorous evaluation to identify and mitigate biases that could lead to disparities in treatment outcomes or perpetuate existing healthcare disparities.
3. The Regulator shall:
 - a. be responsible for enforcing compliance with algorithm transparency, bias mitigation, and informed consent requirements as outlined herein and may authorise regular audits and assessments of AI/ML systems' adherence to transparency, bias mitigation, and informed consent standards to ensure ongoing compliance and accountability;
 - b. collaborate with industry stakeholders to develop guidelines and best practices for scaling AI/ML and blockchain networks in healthcare to ensuring that scalability solutions do not compromise data security or decentralisation principles.



14. FEEDBACK, CONFIDENTIALITY, AND PROTECTION OF WHISTLE-BLOWERS

1. The Regulator will ensure that it has a functional reporting mechanism to allow any person to report illegal or unethical use of health data, unauthorised re-identification as well as feedback on problems or omissions associated with this Act.
2. Any report of unethical or illegal health data to the Regulator shall remain strictly confidential and the identity of the person(s) who provided the report shall only be disclosed with the express consent of the person who provided the report, or as directed by the Tribunal or a court of law.
3. No controller may discriminate in any way, including but not limited to disciplinary or similar steps, against any person who reports illegal or unethical health data practices.

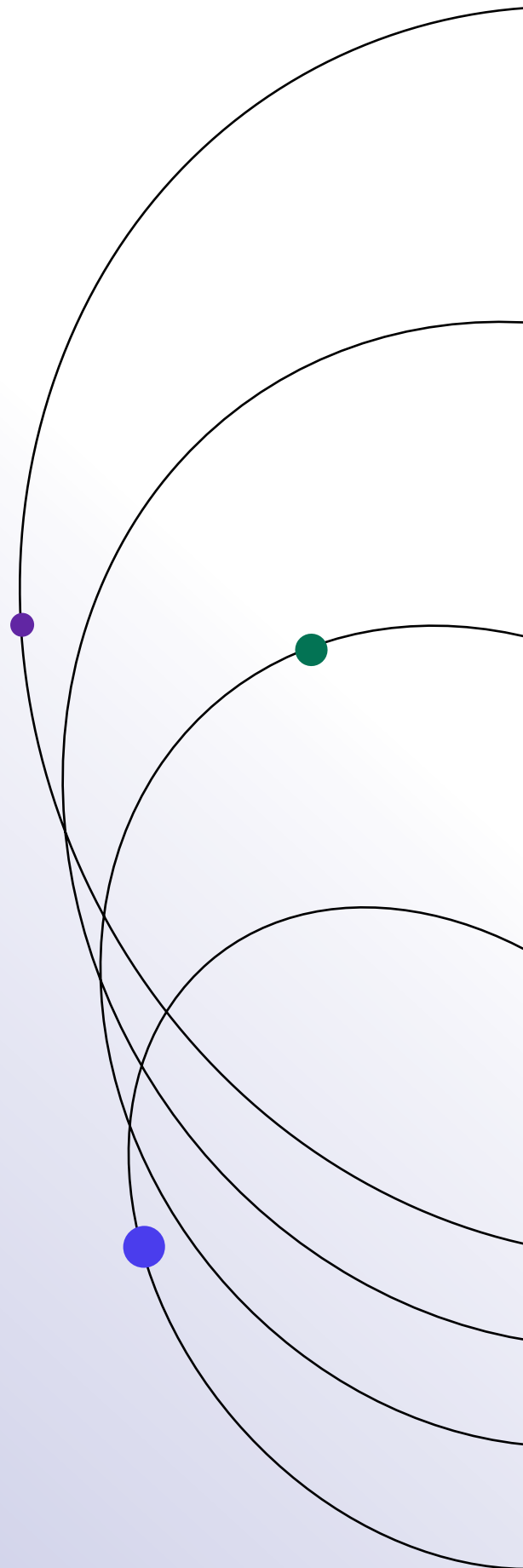
15. RESOLUTION OF DISPUTES AND THE RIGHT OF REDRESS

1. Upon receipt of a complaint, the complainant and the controller must first attempt to remedy any breach of this Act by consulting with all the affected parties in an attempt to find a mutually acceptable resolution, provided that where one of the parties states in writing that the matter is not capable of being resolved by negotiation or mediation then the dispute will be escalated as set out below.
 2. Any person or community, which includes, but is not limited to, the Regulator, that is directly or indirectly affected by an alleged breach of this Act, may commence civil litigation against a party responsible for the said breach.
- 

16. OFFENCES

Any person who commits any of the acts set out hereunder is guilty of an offence:

- a.** Unauthorized access or disclosure: Intentionally accessing or disclosing health data without authorisation or beyond the scope of consent provided by the data subject.
- b.** Gross failure to protect health data: Serious failure to implement adequate security measures, resulting in the unauthorised access, alteration, loss, or destruction of health data.
- c.** Misuse of Data: Using health data for purposes other than those explicitly consented to by the affected person or community or as permitted by law, including unauthorised commercialisation or profiling.
- d.** Non-compliance with Access Rights: Failing to provide persons with access to their health data, or to correct or delete their data as requested and as required by law.
- e.** Obstruction of Oversight: Interfering with or obstructing the work of the Regulator or Tribunal or failing to comply with lawful requests for information, audits, or investigations.
- f.** Falsification of Data: Knowingly altering, falsifying, or destroying health data or related records to deceive or mislead regulatory bodies, data subjects, or other entities.
- g.** Failure to Report Breaches: Not reporting data breaches to the Tribunal and affected data subjects in accordance with the law's requirements.
- h.** Re-identification: Re-identification of Health Data or attempting to re-identify Health Data in contravention of section 10.



17. PENALTIES

1. Controllers or individuals found guilty of committing any of the offences outlined in section 16 may be subject to penalties, including fines, orders for corrective action, suspension, or revocation of licences and criminal prosecution.
2. The severity of penalties will be determined based on the nature of the offence, the harm caused, the offender's intent, and previous compliance history.
3. A person convicted of an offence in terms of this Act is liable, in the case of a contravention of section [insert subsection] to a fine of [amount] or to imprisonment not exceeding [duration] or to both such fine and imprisonment.



18. SUBSIDIARY LEGISLATION

1. The [relevant national authority] is empowered to issue, amend, and repeal [subsidiary legislation] in terms of this Act to ensure its effective implementation, compliance, and enforcement.
2. [Subsidiary legislation] issued in terms of this [Model Law on Health Data Governance] may cover a wide range of areas related to health data governance, including, but not limited to, data protection standards, individual and community rights, controller obligations, reporting requirements, audit procedures, and penalties for non-compliance.
3. The objectives of such [subsidiary legislation] shall be to protect individual and communal privacy, ensure the security of health data, promote ethical data use, enhance data quality and integrity, and facilitate beneficial health data sharing in accordance with the principles and purposes outlined in this [Model Law on Health Data Governance].
4. Before issuing, amending, or repealing [subsidiary legislation] the [relevant national authority] shall ensure that a consultation with interested parties is conducted which is transparent, inclusive, and accessible.

19. REVIEW

1. The Regulator may initiate an impact assessment of this [Model Law on Health Data Governance] at any time, but a mandatory impact assessment of this [Model Law on Health Data Governance] will be initiated by the Regulator at least every [insert number of years] with a view to identifying existing problems as well as technological, legal, or societal changes affecting health data governance.
2. The impact assessment will be delivered to the to the [relevant national authority] and will include any recommended additions, amendments and deletions.

20. TRANSITIONAL PROVISIONS

1. Transitional provisions shall be included in amendment legislation to address the implementation of changes, ensuring a smooth transition for controllers, individuals, and communities affected by the amendments.
2. These provisions may specify grace periods for compliance, outline phased implementation schedules, or provide for the continuation of certain practices under specified conditions.

21. SHORT TITLE AND COMMENCEMENT

1. Short Title:
 - a. This law may be cited as the [Model Law on Health Data Governance].
2. Commencement:
 - a. This [Model Law on Health Data Governance] will be officiated on [specific date], following its authorization by [the president of the country].



APPENDIX A: AMENDMENTS TO DATA PROTECTION LEGISLATION

Law Amended	Amendment
[data protection act]	<p>1. The [data protection act] is hereby amended as follows:</p> <p>a. The Regulator of the [data protection act] is hereby empowered to in terms of the [Model Law on Health Data Governance]to:</p> <ul style="list-style-type: none"> (i) investigate and receive complaints of alleged contraventions of the [Model Law on Health Data Governance]; (ii) enter into cooperation agreements with other governmental bodies that exercise concurrent jurisdiction over health data, controllers or healthcare providers; (iii) assist with the training and education of the public and healthcare providers; (iv) respond to requests for advice from health data holders; (v) mediate disputes between health data holders, communities and individuals with a view to achieving a mutually acceptable solution for all parties; (vi) conduct research into health data governance in order to ensure that health data governance is based on credible evidence; (vii) develop or approve healthcare best practices, certifications and standards which consider interoperability and international best practice; (viii) enter into international agreements with international bodies that have a similar mandate to the Tribunal in order to foster cooperation, health data sharing, security and trust in health data; and (ix) develop safeguards to combat discrimination, bias, stigma and harassment of individuals, communities and controllers relating to the processing of health data

