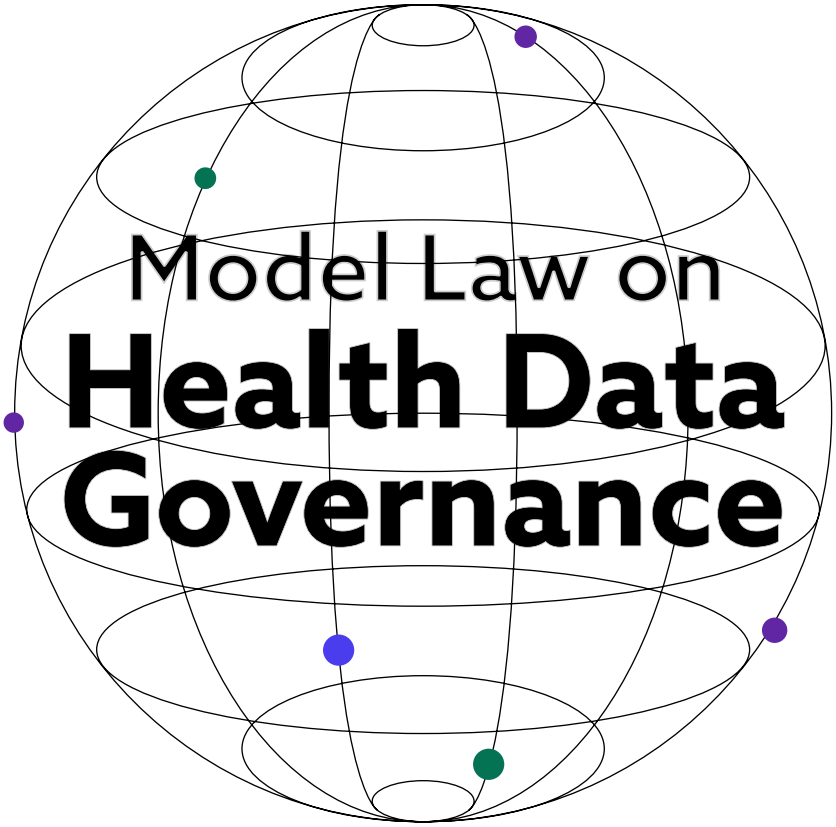
Model Law on Health Data Governance

Health Data Governance Framework

A blueprint for strengthening national legislation



The Health Data Governance Framework was developed by Transform Health. This work was funded by the Patrick J. McGovern Foundation and Fondation Botnar.

Transform Health is a global coalition of organisations that work to harness the potential of digital technology and the use of data to achieve universal health coverage (UHC) by 2030. To learn more about Transform Health visit: www.transformhealthcoalition.org.

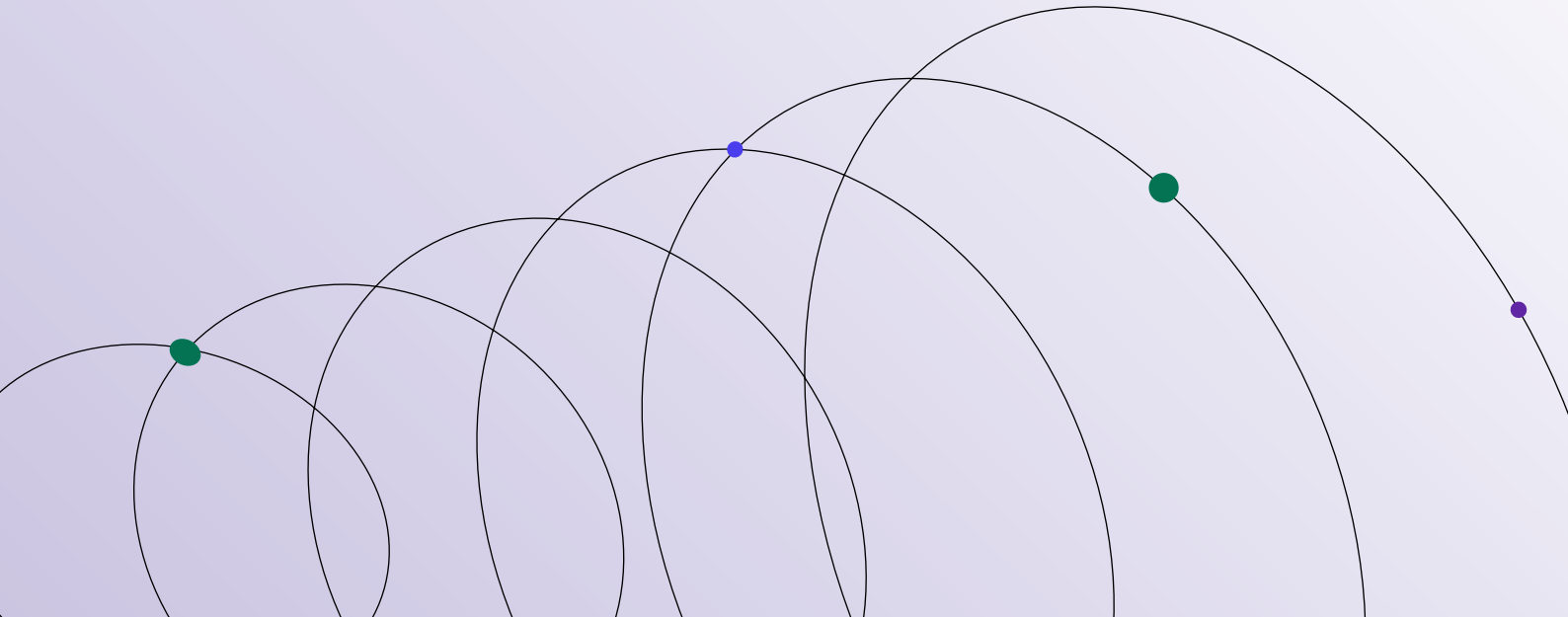
PREFACE

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 use. 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 Health Data Governance Framework

This Health Data Governance Framework 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 Health Data Governance Framework 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.

The law also 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. The Health Data Governance Framework provides the foundation for a global health data governance framework, which, through its endorsement by governments through a World Health Assembly resolution, would build consensus across countries around these core principles and standards that should be addressed through national legislation and regulation for the effective and equitable governance of health data.



Provides non-prescriptive guidance

The primary intention of this Health Data Governance Framework is to **offer guidance to countries aiming to integrate its principles and standards (or relevant sections of the Health Data Governance Framework) into their existing national legislation or develop new laws where and if needed.**

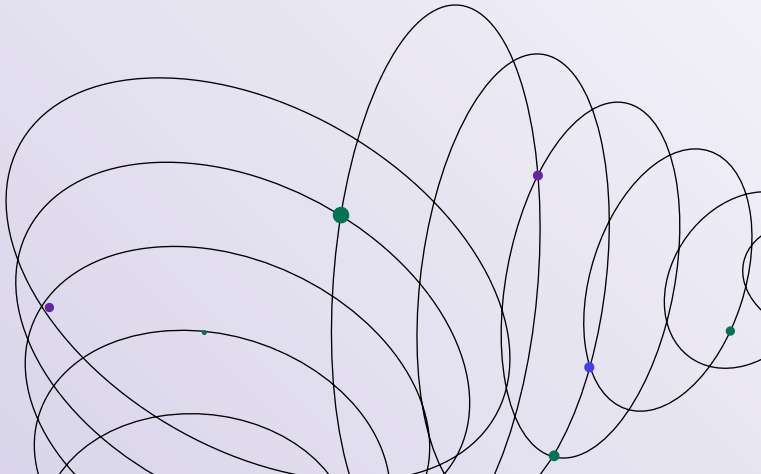
The Health Data Governance Framework is **not meant to be prescriptive** but rather serves as a blueprint, providing a flexible framework that can be adapted to suit the legal systems of different countries. It is not prescriptive or imposing in any way, but rather serves as a legislative guide and a resource to assist countries with their efforts to strengthen their national laws and frameworks dealing with health data governance. This Health Data Governance Framework has been developed to serve as reference text for the drafters of legislation and is not meant to dictate to countries what their health data governance law should be.

Different parts of the Health Data Governance Framework can be inserted into different existing laws within a country, or support the development of new laws. It does not need to be implemented as a single health data governance law. Appendix A provides a structured list of the possible amendments that existing data protection or related laws may need to undergo to effectively provide for the additional duties, powers, and obligations envisioned in this Health Data Governance Framework.

Although this Health Data Governance Framework 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.

Complements existing Data Protection law

This Health Data Governance Framework operates on the assumption that **countries already possess an existing data protection law or data protection regulatory framework** thereby complementing and enhancing the current legal structures, rather than conflicting with them or duplicating efforts. For countries where this is not the case, we strongly recommend that such a framework be developed as a matter of urgency in which case such countries can leverage the many good international practices that exist in this regard. Cognisant of the fact that the nature of digital health infrastructure and regulatory frameworks may differ between countries, this Health Data Governance Framework also tries to accommodate 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. To prevent duplication of existing national regulations pertaining to issues such as informed consent or individual rights and obligations with regard to data, this Health Data Governance Framework assumes the existence of a data protection law in any given national jurisdiction that deals with the basic data protection rights and obligations of individuals. Accordingly, only health data governance issues that are not usually dealt with in standard data protection laws are being addressed in this Health Data Governance Framework.



Choice of a Health Data Governance Framework as an instrument

While principles provide broad guidance, a Health Data Governance Framework lays out specific legal provisions, definitions, and mechanisms that can be directly incorporated or customised to fit within existing national laws. Countries can implement parts of this Health Data Governance Framework or take inspiration from the provisions contained in it.

In comparison with related regulatory instruments such as guidelines, policies, or checklists, a Health Data Governance Framework was the preferable instrument for the procurement of goods, construction, and services.[1] There are several examples of the use of a Health Data Governance Framework as an instrument, at both regional and international levels, such as the UNCITRAL Health Data Governance Framework on Electronic Transferable Records[2], AU Health Data Governance Framework on Medical Products Regulation[3] , the Health Data Governance Framework on Access to Information for Africa[4], among others. In the context of health data governance, the advantages of using a Health Data Governance Framework "template" over any other regulatory instrument include the following:

- **Flexibility:** Health Data Governance Frameworks 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 including specific components of it to their specific needs while still maintaining consistency with international standards.
- **Harmonisation:** Health Data Governance Frameworks facilitate the harmonisation of laws across different jurisdictions. By providing a common framework, Health Data Governance Frameworks help to reduce legal inconsistencies and barriers to international health data sharing.
- **Efficiency:** Health Data Governance Frameworks 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:** Health Data Governance Frameworks promote international cooperation by providing a basis for countries to work together in developing common legal standards informed by globally agreed principles, existing good practices and emerging needs. 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 endorsing a Health Data Governance Framework, 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 data controllers, leading to increased confidence in the health data governance space.

Overall, a Health Data Governance Framework 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 Health Data Governance Framework as a Global Standard. International and Comparative Law Quarterly. 2004;53(1):17-46. doi:10.1093/iclq/53.1.17

2 Available at: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records

3 Available at: https://www.nepad.org/publication/au-model-law-medical-products-regulation

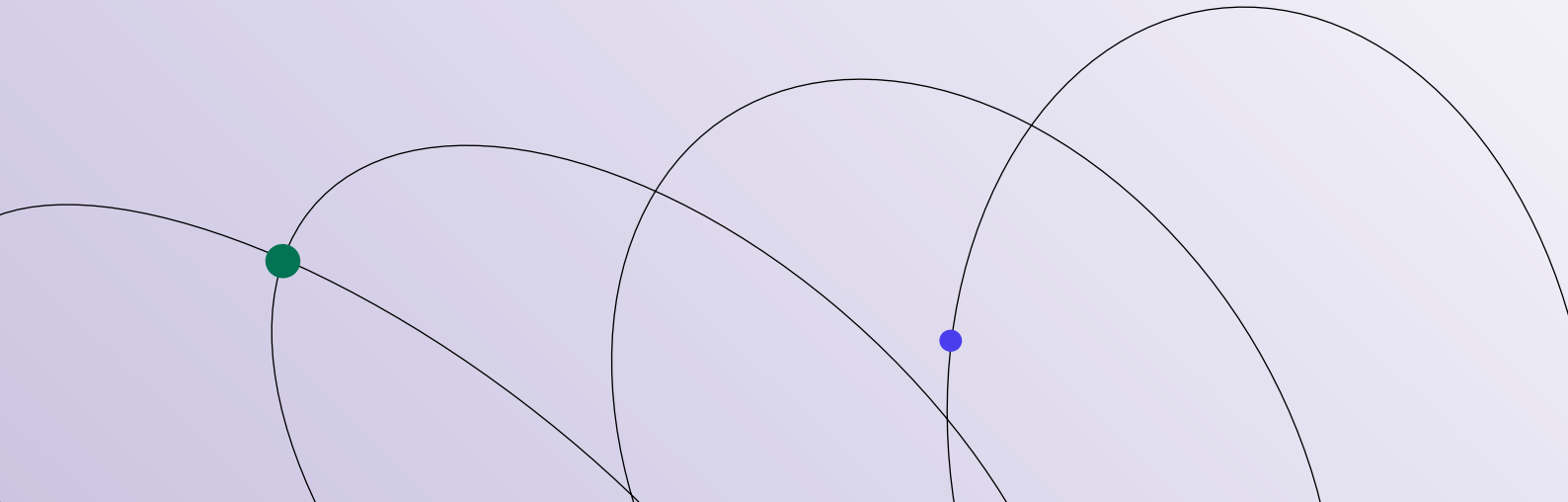
4 Available at: https://achpr.au.int/en/node/873

Government endorsement of the Health Data Governance Framework

The **endorsement of this Health Data Governance Framework by Member States through a World Health Assembly (WHA) resolution and regional mechanisms**, can provide a platform for member states to discuss, evaluate, and agree on core areas that should be addressed in national legislation. While a WHA resolution itself does not have direct legislative authority over individual countries, its endorsement by Member States would show political commitment and agreement around the core areas contained in the Health Data Governance Framework. The practical impact of a WHA resolution for individual countries would include the establishment of a global standard for health data governance legislation, providing of guidance and best practices for countries to follow when strengthening their own health data governance frameworks, the protection of individual and community rights, the facilitation of interoperability between health systems and data sharing across borders, 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. Moreover, **a Health Data Governance Framework can help to 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.

Development of the Health Data Governance Framework

This draft Health Data Governance Framework has been informed by equity and rights-based health data governance principles (endorsed by more than 150 organisations and governments) and draws inspiration from the OECD Recommendation on Health Data Governance (adhered to by 38 OECD member countries), 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, instruments 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, and reports.



The process to inform the development of a draft of the Health Data Governance Framework for public consultation also included seven regional multi-stakeholder consultations (convened by Asia eHealth Information Network/AeHIN, Pan African Health Informatics Association/HELINA and RECAINSA), which consulted more than 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. This was followed by a public consultation period on the draft between the 7th and 30th of April 2024, which engaged more than 550 stakeholders and experts from more than 35 countries, including from government, UN and other multilateral agencies, civil society organisations, youth representatives, academia, parliamentarians, regulatory bodies, among others. The public consultations period entailed the wide dissemination of the Health Data Governance Framework and feedback survey in five languages, 14 national and regional consultations (organised by Transform Health, AeHIN, HELINA, RECAINSA), two youth consultations, and expert interviews.

The drafting of the Health Data Governance Framework has been led by a legal team specialising in data governance law and has been shaped by inputs from the Africa CDC Flagship Initiative on Health Data Governance and the Transform Health Policy Circle and other working groups. An advisory group was set up to provide expert guidance and feedback on the Health Data Governance Frameworks, which included representatives from OECD, Resolve to Save Lives, the University of St. Gallen (HSG), the University of Copenhagen (Department of Public Health), the University of Vienna (Department of Political Science), Palladium Group, Instituto De Efectividad Clínica Y Sanitaria (IECS), WHO, PharmAccess, Transform Health and ETH Zürich Health Ethics and Policy Lab.

Cross border data flows

The governance of cross border data flows is usually extensively governed in national data protection laws and in keeping with the premise that this Health Data Governance Framework is building on existing national data protection laws, this Health Data Governance Framework only deals with cross border data flows to a limited extent and with issues related to this that are not usually being dealt with in national data protection laws. Moreover, given that the Health Data Governance Framework provides a template for national legislation, it does not establish a framework for cross-border data sharing. Such a framework or agreement to operationalise cross-border data sharing would need to be negotiated between countries.

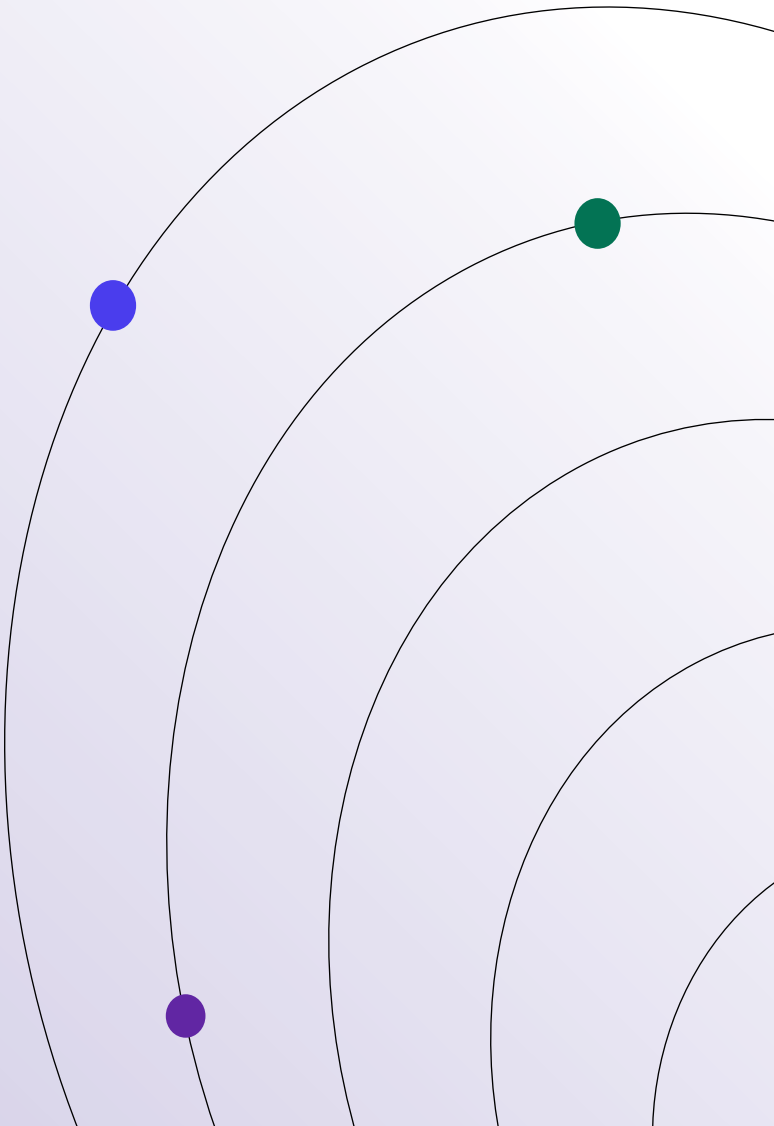


TABLE OF CONTENTS

1. PURPOSE

1. This [Health Data Governance Framework on Health Data Governance] **acknowledges the special nature of health data**, recognising its significant implications for individual privacy and healthcare, community identity, heritage, cultural practices, and collective health, as well as its critical role in advancing research and innovation in healthcare and preventing and responding to health emergencies.
2. This [Health Data Governance Framework on Health Data Governance] augments [Data Protection Law] **by addressing unique aspects of health data,** aiming to effectively balance the interests of individual data subjects, their communities, and the health research community.
3. To accomplish the general purposes outlined in subsections (1) and (2), this [Health Data Governance Framework on Health Data Governance] sets forth the following specific aims:

    a. **Create effective governance structures to ensure that health data is processed in accordance with the rights and duties** set forth in this [Health Data Governance Framework on Health Data Governance], and that disputes are resolved by a specialised judicial forum.

    b. **Confirm, expand on, and better safeguard individual privacy rights** in personal health data.

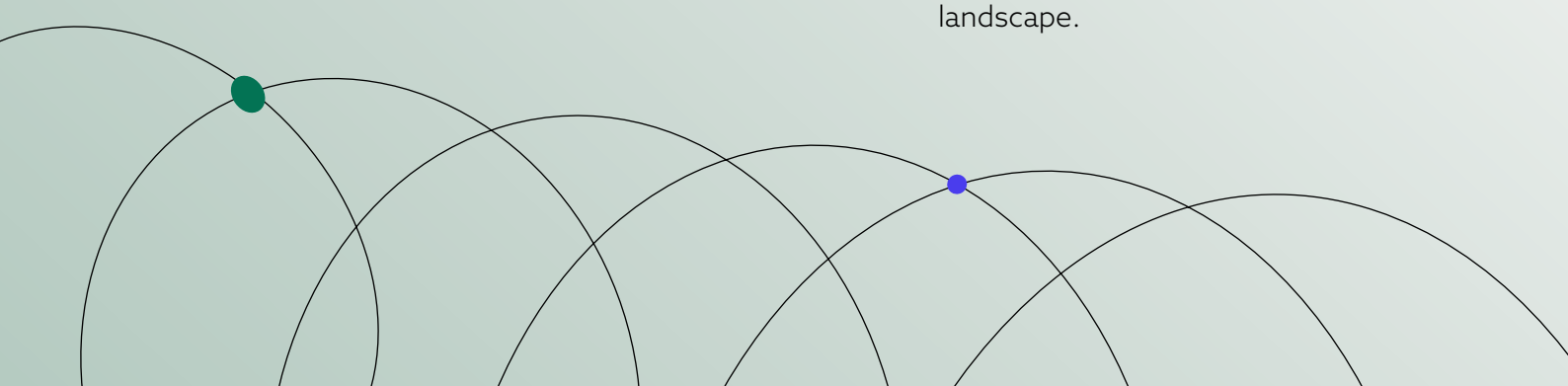
    c. **Establish a system to protect the interests of communities in health data** that contain information that is significant to their identity, heritage, cultural practices, or collective health.

    d. **Foster an environment conducive to health research and innovation** by recognising and protecting the proprietary rights of individuals and entities that invest in generating health data as part of their regular business or professional activities.

    e. Ensure that health data generated by government departments or agencies that **does not identify individuals** is managed as a public good by making it open access.

    f. **Implement mechanisms to enable health data sharing**, such as mandated transparency and the provision of compulsory use-licenses for health data, when justified by the public interest.

    g. **Provide a flexible and adaptive legal framework that accommodates 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

1. In this [Health Data Governance Framework on Health Data Governance], unless the context clearly indicates otherwise, the following terms have the corresponding meanings:

   a. **"Anonymisation"** means the process of irreversibly transforming personal health data into a form in which the individual to whom the data relates cannot reasonably be identified, directly or indirectly, while still allowing the data to be used for legitimate purposes. "**Anonymised"** has a corresponding meaning;

   b. **"Community"** means a group of individuals 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. **"Consent"** is as defined in the [Data Protection Law] but is extended to include communities as contemplated in section 9;

   e. **"Data controller"** means the individual or entity responsible for determining the purposes and means of the processing of health data;

   f. **"Data subject"** means the identified or identifiable individual to whom personal health data relate;

   g. **"Electronic medical record"** means a digital collection of a patient's medical history, treatments, diagnoses, laboratory testing results, immunisations, and other health-related information maintained and held by a healthcare provider;

   h. **"Emerging technologies"** means novel and rapidly evolving tools, systems, and methodologies that harness computational advancements, data science or biomedical research to transform healthcare delivery, management, and decision-making. These technologies may include, but is not limited to, innovative computational models, artificial intelligence, machine learning, blockchain, and big data analytics.

   i. **"Entity"** means a juristic person;

   j. **"Healthcare provider"** means any individual or entity 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;

   k. **"Health data"** means data related to human health, irrespective of whether such data can identify such individual or not and includes personal-level data, population-level data, facility data, and system data that relate to human health;

   l. **"Health-related data"** means data that is not directly connected to the human health, but can by indirect means be used to make conclusions about health data;

m. **"Health Data Court"** means the Health Data Court as created by this [Health Data Governance Framework on Health Data Governance] in section 6;

n. **"Health data generator"** means any individual or entity that, as part of their business or professional activities, collects, creates, sequences, or otherwise generates health data, including through the instruction of automated means, and stores such health data in a digital format;

o. **"Individual"** means a natural person;

p. **"Non-identifying health data"** means health data that either is inherently non-personal, such as population-level data, or has been anonymised or pseudonymised to remove personal identifiers. As such, this type of health data cannot legally be used by an unauthorised individual or entity to identify a data subject.

q. **"Personal health data"** means health data which is inherently sensitive and that relate to an identified or identifiable individual; an identifiable individual 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 individual;

r. **"Processing"** means any operation, activity, or any set of operations, whether or not by automated means, concerning health data;

s. **"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 individual 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 individual. "Pseudonymised" has a corresponding meaning;

t. **"Public interest"** means a potential health benefit, such as a better medicine or diagnostic tool, for the entire population or any group of individuals, whether big or small, in [Country];

u. **"Re-identification"** means the process by which information is attributed to anonymised or pseudonymised personal health data in order to identify the individual or community to whom the de-identified data relate

v. **"Regulator"** means the government agency responsible for the implementation of the [Data Protection Law];

w. **"Relevant national authority"** means the member of the national executive responsible for the administration of this [Health Data Governance Framework on Health Data Governance].

3. SCOPE

1. This law applies to all individuals and entities involved in the collection, generation, processing, storage, use, access, sharing and disposal of health data and health-related data. This includes, but is not limited to, healthcare providers, health insurance companies, health information technology companies, holders of proprietary rights in digital instances containing health data, data controllers, 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], including the processing of such data-by-data controllers located outside [Country] if the data pertains to individuals and/or communities within [Country].

4. EXCLUSIONS

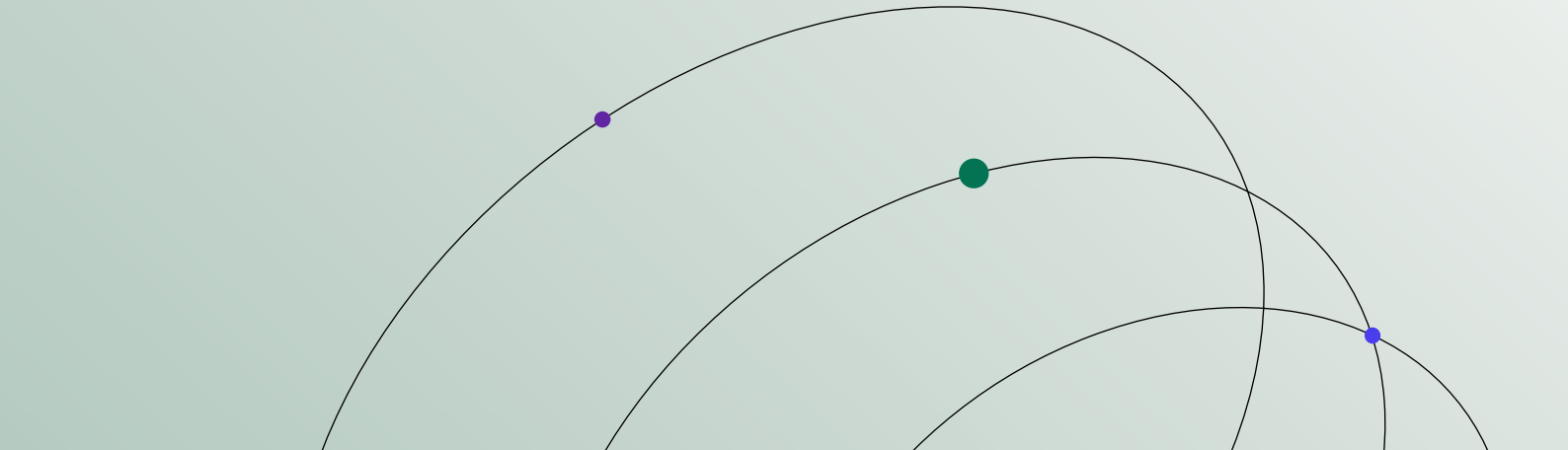
1. This [Health Data Governance Framework on Health Data Governance] does not apply to:
    a. health data collected, processed, stored, or used for personal or household activities with no connection to a public or professional context;
    b. personal data which is not health data or health-related data;
    c. health data which is required by a public body which is aimed at assisting in the identification and financing of terrorist and related activities, money laundering, defence or public safety provided that any public body must first obtain an exemption from this [Health Data Governance Framework on Health Data Governance] based on this section from the Regulator and provided that the exemption must be clearly defined, necessary and proportionate and where the failure to provide the exemption will prejudice the legitimate aim of the public body;
    d. journalistic, literary or artistic expression;
    e. the judicial functions of a court.

5. INTERPRETATION

1. The use in this [Health Data Governance Framework on Health Data Governance] 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 conveying legal ownership or proprietary rights.
2. Where this [Health Data Governance Framework on Health Data Governance] refers to consent or other legal actions by individuals, for those individuals who legally cannot perform such actions on their own, such as minors, these actions shall be conducted as specified under the [Data Protection Law].
3. This [Health Data Governance Framework on Health Data Governance] is intended to augment the existing [Data Protection Law], create the Health Data Court and expand the duties of the Regulator created in terms of the [Data Protection Law]. Where this [Health Data Governance Framework on Health Data Governance] is silent, reference should be had to the existing provisions of the [Data Protection Law]. In the event of a conflict between the [Data Protection Law] and this [Health Data Governance Framework on Health Data Governance], this [Health Data Governance Framework on Health Data Governance] will prevail.

6. HEALTH DATA COURT

1. This law establishes the Health Data Court to adjudicate matters related to the governance, use, and protection of health data within [Country].
2. The objective of the Health Data Court is to ensure the fair, transparent, and efficient resolution of disputes arising under this [Health Data Governance Framework on Health Data Governance].
3. The Health Data Court shall have jurisdiction over all matters arising under this [Health Data Governance Framework on Health Data Governance], including disputes between the Regulator, individuals, communities, data controllers, and holders of proprietary rights in digital instances containing health data, including the imposition of penalties for violations.
4. The Health Data Court is empowered to hear cases, make determinations, order remedial actions, impose penalties, and take any other actions deemed necessary to enforce the provisions of this [Health Data Governance Framework on Health Data Governance].



5. The Health Data Court shall consist of [a specified number] of judges, with expertise in health data management, law, ethics, and technology.

6. Judges of the Health Data Court 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 Health Data Court 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 Health Data Court can be appealed to [the higher court or body] within [number] days of the decision, on matters of law or jurisdictional error.

9. The Health Data Court can make any order in the same manner and to the same extent as the [high court]. Failure to comply with a decision of the Health Data Court constitutes an offence under this [Health Data Governance Framework on Health Data Governance].

10. The Health Data Court shall be funded by [source of funding], and shall have access to the necessary resources, staff, and facilities to effectively carry out its functions.

11. Data controllers, communities, individuals, and holders of proprietary rights in digital instances containing health data have the right to appeal against decisions made by the Regulator regarding the determination of offenses and the imposition of penalties, through judicial review or other legal mechanisms provided by law.

12. In addition to penalties, offenders may be required to provide restitution to affected data subjects, compensating them for any harm caused by the offense.

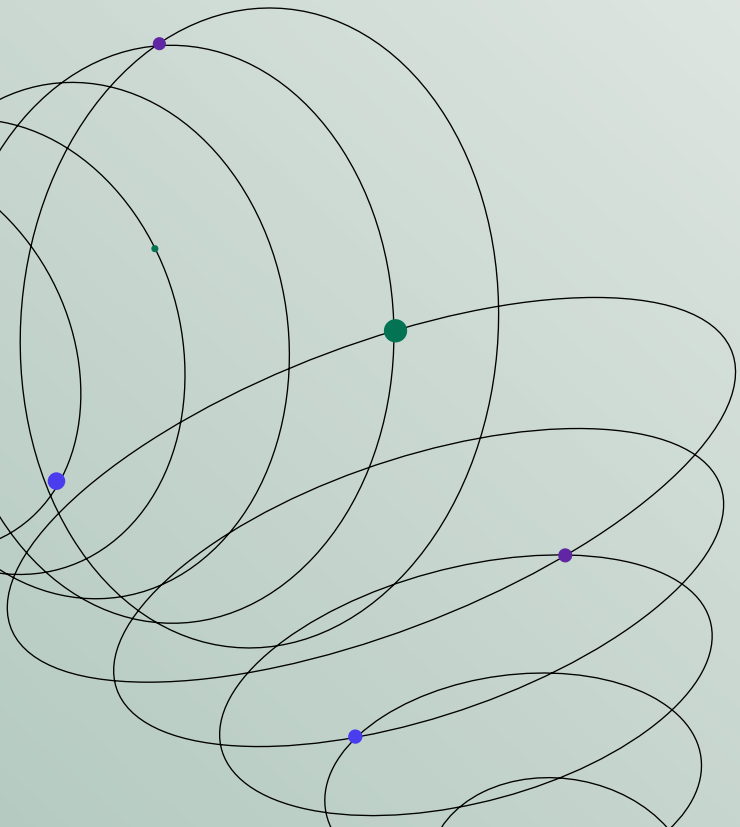
13. The Health Data Court may also order remedies, including the implementation of specific measures to rectify violations and prevent their recurrence.

14. 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.

15. Any individual, entity, or community that suffers damages as a result of a breach of this [Health Data Governance Framework on Health Data Governance] may commence civil litigation against a party responsible for the said breach in the Health Data Court for damages and/or compliance with this [Health Data Governance Framework on Health Data Governance].

7. INDIVIDUAL RIGHTS; PORTABILITY OF ELECTRONIC MEDICAL RECORDS

1. All individuals have privacy rights in their personal health data as provided for in [existing data protection legislation].
2. In addition, individuals have the right to portability of electronic medical records, which means that a healthcare provider that holds an electronic medical record of an individual, shall, upon request by the individual to transfer his or her electronic medical record to another specified healthcare provider, located either in [Country] 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. PROHIBITION ON RE-IDENTIFICATION

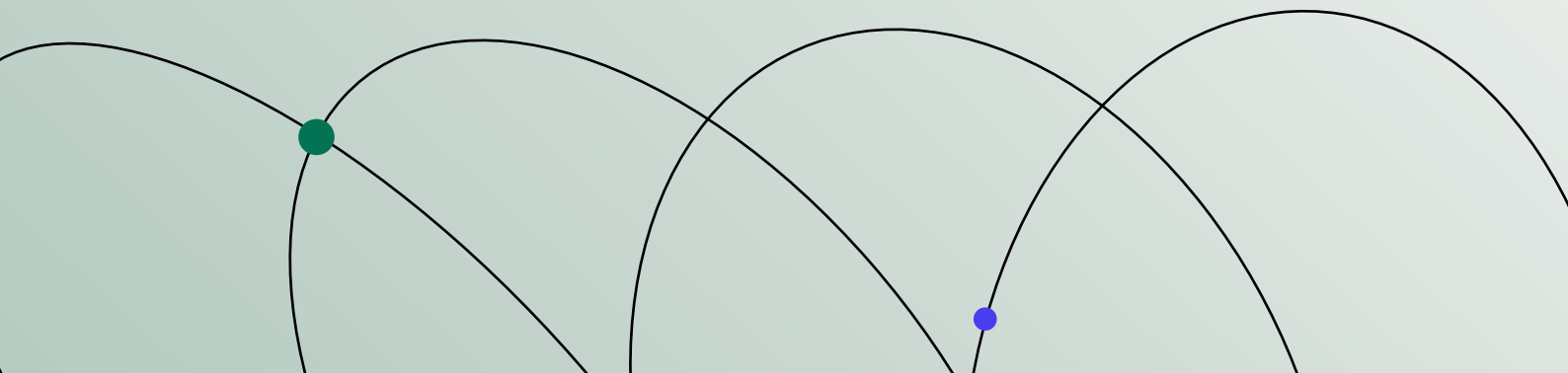
1. Subject to subsection (2), no one who obtains, possesses, or has access to anonymised or pseudonymised personal health data shall intentionally engage in any action with the purpose or effect of re-identifying the said data.
2. Where the holder of proprietary rights in digital instances containing personal health data has such personal health data anonymised or pseudonymised, the holder can authorise individuals or entities to conduct tests of the robustness of the anonymisation or pseudonymisation processes.
3. Any individual or entity that, 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 holder of proprietary rights in digital instances containing such health data and the Regulator within [specified timeframe].
4. Upon receiving information regarding potential re-identification risks, the holder of proprietary rights in digital instances containing such health data 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.
5. The Health Data Court may, upon good reasons provided, lift the prohibition in subsection (1) with respect to specified health data, and subject to the conditions that the Health Data Court may determine.

9. COMMUNITIES' RIGHTS IN THEIR COMMUNITY HEALTH DATA

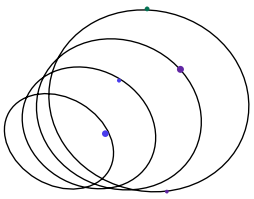
1. A community shall act through its representative body for purposes of this [Health Data Governance Framework on Health Data Governance].
2. The [relevant national authority] shall establish transparent mechanisms in subsidiary legislation regarding:
    a. the criteria for an individual or individuals to be recognised as the representative body of a community for purposes of this [Health Data Governance Framework on Health Data Governance], and
    b. for supporting the effective functioning of representative bodies.
3. A data controller may only process a community's community health data if such community consents 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 Health Data Court to review the decision of the representative body in terms of [existing administrative law legislation / the common law principles of administrative justice].
8. A data 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.

10. RIGHTS AND OBLIGATIONS OF HEALTH DATA GENERATORS; OPEN ACCESS TO BE PROVIDED BY THE STATE

1. By virtue of collecting or generating health data and storing such health data in digital format, a health data generator obtains transferable proprietary rights in the digital instances containing such health data, provided that:
    a. if such proprietary rights are in conflict with an individual's privacy rights as contemplated in section 7, the individual'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 9.
    c. Where an individual or entity that holds any proprietary rights as contemplated in this subsection have duties in terms of [Data Protection Law], such individual or entity shall enforce such proprietary rights to fulfil such duties.
2. The state must provide open access to the general public to all digital instances of non-identifying health data that are owned by any government department or agency, provided that if any such data is also community health data, the state must first comply with section 9 in respect of such data.
3. The state must take reasonable administrative measures, within its available resources, to support such open access. This includes:
    a. cataloguing such data,
    b. ensuring its publication, facilitating barrier-free and cost-free access,
    c. where relevant, ensuring compliance with section 9, and
    d. ensuring that all data shared in terms of this section complies with interoperability standards as determined by the Regulator.



11. USING HEALTH DATA IN THE PUBLIC INTEREST



1. Any individual or entity shall, upon request by anyone else, disclose whether they have any proprietary rights related to health data.
2. The [relevant national authority] may through subsidiary legislation exclude any class of individuals or entities from the operation of subsection (1).
3. An individual or entity that has proprietary rights related to health data shall, upon request by anyone else, 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 individual or entity, hereinafter referred to as 'the applicant', may apply to the Health Data Court 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 if this section, the Health Data Court 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 holder of proprietary rights in digital instances containing health data for refusing access, common practice in the relevant market, and any potential harm or risks to the individuals and communities.
6. The Health Data Court may determine a reasonable licence fee to be paid by the applicant to the holder of proprietary rights in digital instances containing health data 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 Health Data Court deems relevant.
7. The Health Data Court 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 Health Data Court 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 Health Data Court 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. PANDEMICS AND OTHER HEALTH EMERGENCIES

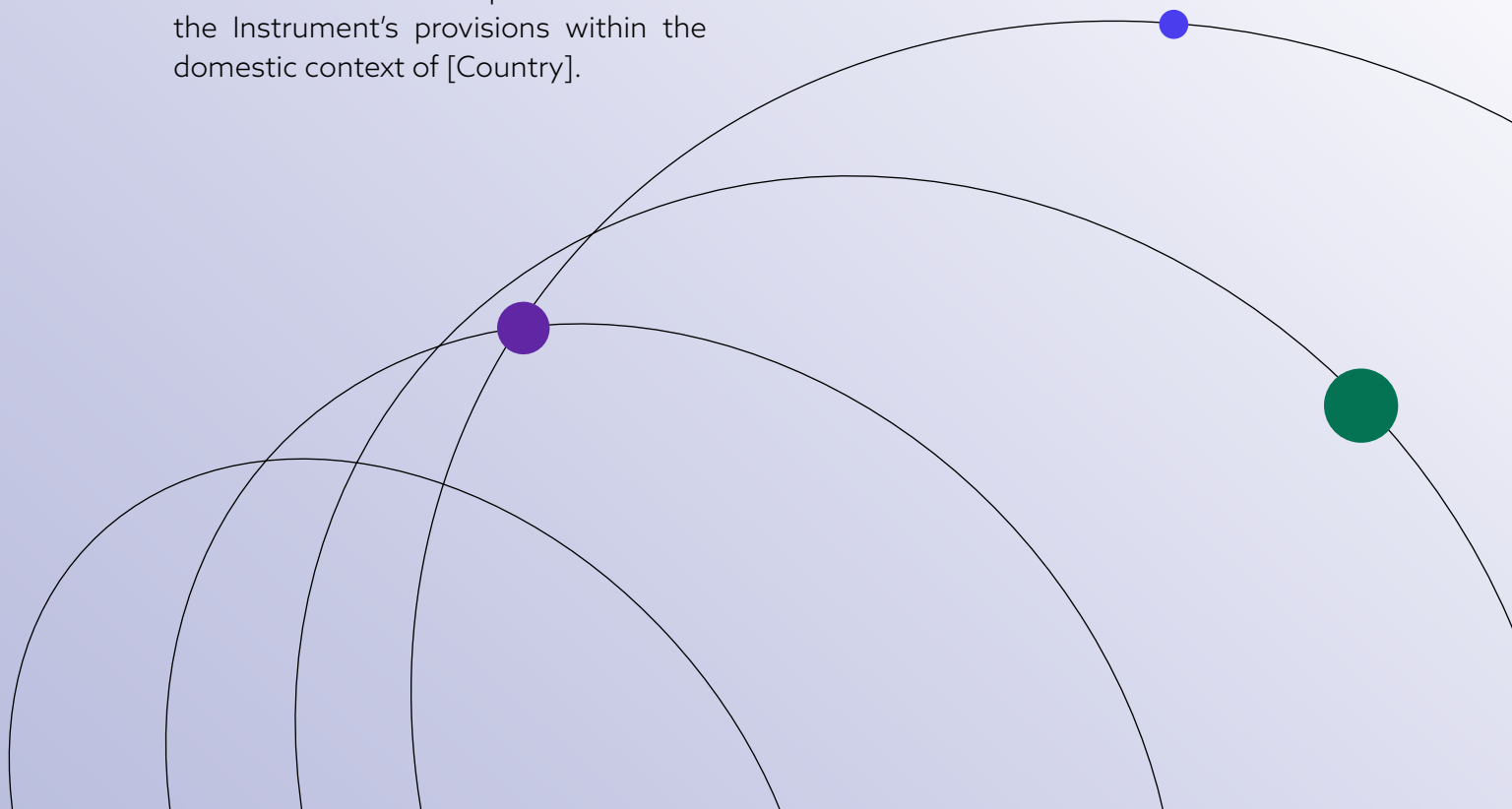
1. Upon ratification by [Country] of the Pandemic Prevention, Preparedness and Response Instrument (the "Instrument"), as drafted and negotiated through the intergovernmental negotiating body, for endorsement by Member States at the Seventy-seventh World Health Assembly, in May 2024, the provisions contained within the Instrument shall be deemed incorporated in the domestic law of [Country] and shall enter into force on a date promulgated by the [relevant national authority].

2. Prior to the promulgation of the effective date:

    a. the [relevant 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.

3. Following the promulgation of the effective date, and to the extent that the Instrument applies to health data, the Regulator shall be empowered to issue directives and guidelines for the effective implementation of the Instrument'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, which information must allow such individuals or communities to provide informed consent as described in section 9 above.

2. All emerging technologies 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 relevant emerging technology 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 the systems of emerging technologies for 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 emerging technologies in healthcare to ensuring that scalability solutions do not compromise data security or decentralisation principles.

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

1. The Regulator will ensure that it has a functional reporting mechanism to allow anyone to report illegal or unethical use of health data, unauthorised re-identification as well as feedback on problems or omissions associated with this [Health Data Governance Framework on Health Data Governance].

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 Health Data Court or a court of law.

3. No data 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. OFFENCES

1. Any individual or entity that 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 data subject or affected community or as permitted by law, including unauthorised commercialisation or profiling.

    d. non-compliance with access rights; failing to provide individuals with access to their health data, or to correct or delete their data as requested and as required by law.

    e. failure to provide health data when instructed to do so by the Health Data Court.

    f. obstruction of oversight; interfering with or obstructing the work of the Regulator or Health Data Court or failing to comply with lawful requests for information, audits, or investigations.

    g. falsification of data; knowingly altering,falsifying, or destroying health data or related records to deceive or mislead regulatory bodies, data subjects, or other entities.

    h. failure to report breaches; not reporting data breaches to the Health Data Court and affected data subjects in accordance with the law's requirements.

    i. re-identification of health data or attempting to re-identify health data in contravention of section 8.

16. PENALTIES

1. Data controllers or individuals found guilty of committing any of the offences outlined in section 15 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. An individual or entity convicted of an offence in terms of this law is liable, in the case of a contravention of section [insert subsection] to a fine of [amount] or, in the case of an individual, to imprisonment not exceeding [duration] or to both such fine and imprisonment.

17. SUBSIDIARY LEGISLATION

1. The [relevant national authority] is empowered to issue, amend, and repeal [subsidiary legislation] in terms of this law to ensure its effective implementation, compliance, and enforcement.
2. [Subsidiary legislation] issued in terms of this [Health Data Governance Framework 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, data 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 [Health Data Governance Framework 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.

18. REVIEW

1. The Regulator may initiate an impact assessment of this [Health Data Governance Framework on Health Data Governance] at any time, but a mandatory impact assessment of this [Health Data Governance Framework 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 [relevant national authority] and will include any recommended additions, amendments, and deletions.

19. TRANSITIONAL PROVISIONS

1. Transitional provisions shall be included in amendment legislation to address the implementation of changes, ensuring a smooth transition for data 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.

20. SHORT TITLE AND COMMENCEMENT

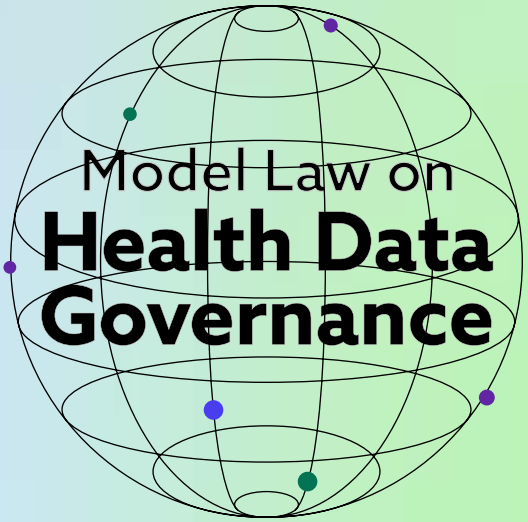
1. Short Title:
    a. this law may be cited as the [Health Data Governance Framework on Health Data Governance].
2. Commencement:
    a. this [Health Data Governance Framework] will be officiated on [specific date], following its authorization by [the head of state of the Country].

APPENDIX A: AMENDMENTS TO [DATA PROTECTION LAW]

The Health Data Governance Framework proposes possible additions or changes to the existing duties, powers, and obligations of government agencies responsible for the implementation of their national Data Protection Law – referred to in this model as Regulators. The aim of this Appendix is to provide a structured list of the possible amendments that existing data protection or related laws may need to undergo to effectively provide for the additional duties, powers, and obligations envisioned in this Health Data Governance Framework.

Law Amended	Amendment
[Data Protection Law]	**1.** The [Data Protection Law] is hereby amended as follows: **a.** The Regulator is hereby empowered and obliged in terms of the [Health Data Governance Framework on Health Data Governance] to: **(i)** investigate and receive complaints of alleged contraventions of the [Health Data Governance Framework on Health Data Governance]; **(ii)** enter into cooperation agreements with other governmental bodies that exercise concurrent jurisdiction over health data, holders of proprietary rights in digital instances containing health data, 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 data controllers; **(v)** mediate disputes between holders of proprietary rights in digital instances containing health data, data controllers, 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 any equivalent body in a foreign state that have a similar mandate to the Regulator in order to foster cooperation, health data sharing, security, and trust in health data; and

Law Amended	Amendment
[Data Protection Law]	**(ix)** develop safeguards to combat discrimination, bias, stigma and harassment of individuals, communities and data controllers relating to the processing of health data; **(x)** provide oversight on matters related to the ethical use, privacy, cross-border transfer, and security of health data; **(xi)** publish annual reports on its activities, decisions, and the state of health data governance within [Country], while respecting confidentiality and privacy obligations; **(xii)** initiate litigation to enforce the provisions of this [Health Data Governance Framework on Health Data Governance]. **b.** The Regulator is hereby empowered and obliged in terms of the [Health Data Governance Framework on Health Data Governance] to create a single designated point of contact which is designed to facilitate international cooperation and mutual assistance with regard to international transfer of health data. **c.** Subject to ratification by [national legislature] the Regulator may enter into any agreement with any equivalent bodies in any foreign state regarding: **(i)** mutual assistance with regard to cross-border transfer of health data, **(ii)** the use of common interoperability standards as required by section 7; **(iii)** the ability of foreign nationals to request licences in terms of section 11; **(iv)** the establishment of points of contact for data sharing, such as data trusts. **(vi)** conduct research into health data governance in order to ensure that health data governance is based on credible evidence; **d.** The Regulator must, as soon as practicable after [national legislature] has agreed to the ratification thereof, assession to, amendment of or revocation of an agreement as set out in sub-section (c) above, publish a notice thereof.



Model Law on Health Data Governance