



# Health Data Governance *Principles*

Universalising the benefits  
of health digitalisation

PROTECT PEOPLE | PROMOTE HEALTH VALUE | PRIORITISE EQUITY

# INTRODUCTION

The Health Data Governance Principles, presented here, bring a human rights and equity lens to the use of data within and across health systems. They are oriented towards supporting sustainable and resilient public health systems that can deliver Universal Health Coverage (UHC).

At the United Nations High-Level Meeting on Universal Health Coverage in 2019, world leaders reaffirmed their Sustainable Development Goal commitment to extend UHC to all people by 2030. Digital health and data-driven health systems can help strengthen the delivery, quality and equity of health services, providing an important opportunity to accelerate progress towards UHC. UHC – and the values of equity and human rights that

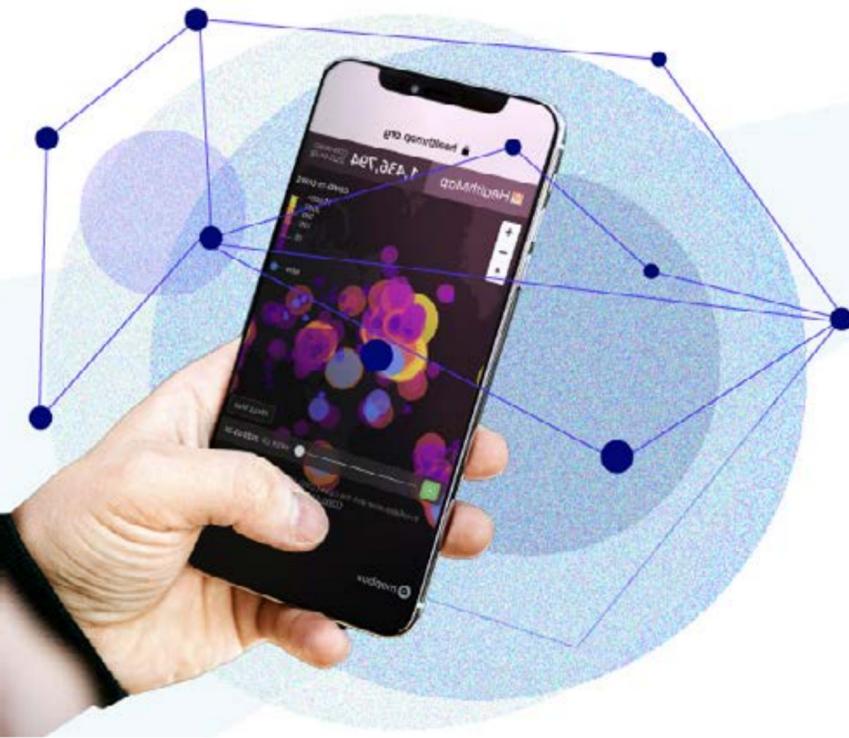
underpin it – must be at the core in the design and development of data-driven health systems.

Data-driven approaches are increasingly either the norm or the aspiration in the operation of health systems and provision of health services. The collection, processing, storage, analysis, use, sharing and disposal of health data has grown in complexity. The COVID-19 pandemic has accelerated the use of data. This exponential increase in data use necessitates robust and equitable governance of health data. Countries and regions around the world are instituting health data governance policies and legislation. However, there is not yet a comprehensive, global set of principles to guide the governance

of health data across public health systems and policies. The Health Data Governance Principles respond to that need.

The Principles are meant to inform and strengthen governance models, instruments, treaties, regulations and standards across countries and regions around a shared vision of equitable health data governance. They are a tool to support the use of digital technologies and data for the health and well-being of all. They are a critical step towards a global framework for health data governance.

The Health Data Governance Principles recognise and build on existing norms, principles, treaties, conventions, and guidelines, including: the [World Health](#)



Organization (WHO)'s data principles<sup>1</sup> (a framework for data governance for WHO) and their guidance on the ethics and governance of artificial intelligence for health<sup>2</sup>; the Principles for Digital Development<sup>3</sup> and Digital Investment Principles<sup>4</sup> stewarded by the Digital Impact Alliance; the Organisation for Economic Co-operation and Development (OECD)'s Recommendation on Health Data Governance<sup>5</sup> and their Principles on Artificial Intelligence<sup>6</sup>; the Pan American Health Organization (PAHO)'s

Principles for Digital Transformation of Public Health<sup>7</sup>; the report of the Lancet and Financial Times Commission on Governing Health Futures<sup>8</sup>; the Universal Declaration of Human Rights<sup>9</sup>; the International Covenant on Economic, Social and Cultural Rights<sup>10</sup>; the International Covenant on Civil and Political Rights<sup>11</sup> and the associated Siracusa Principles on the Limitation and Derogation Provisions<sup>12</sup>. The Health Data Governance Principles are informed by these efforts, while further strengthening the health data governance ecosystem.

<sup>1</sup> World Health Organization Data Principles. Geneva: WHO; 2020 (<https://www.who.int/data/principles>, accessed 5 May 2021).

<sup>2</sup> Ethics and governance of artificial intelligence for health: WHO guidance. Geneva: WHO; 2021 (<https://www.who.int/publications/i/item/g789g240029200>, accessed 5 May 2021).

<sup>3</sup> Principles for Digital Development. Digital Impact Alliance (<https://digitalprinciples.org>, accessed 5 May 2021).

<sup>4</sup> The Principles of Donor Alignment for Digital Health. Digital Impact Alliance (<https://digitalinvestmentprinciples.org>, accessed 5 May 2021).

<sup>5</sup> OECD, Recommendation of the Council on Health Data Governance. OECD; 2016 (<https://www.oecd.org/els/health-systems/health-data-governance.htm>, accessed 12 May 2021).

<sup>6</sup> OECD Artificial Intelligence Principles. OECD; 2019 (<https://oecd.ai/en/ai-principles>, accessed 12 May 2021).

<sup>7</sup> 8 Principles for Digital Transformation of Public Health. Washington: PAHO; 2021 (<https://www.paho.org/en/ish/8-principles>, accessed 20 October 2021).

<sup>8</sup> Kickbusch, I; Piselli, D; Agrawal, A; et al. The Lancet and Financial Times Commission on governing health futures 2030: growing up in a digital world. Lancet. 2021; 398: 1727-1776.

<sup>9</sup> Universal Declaration of Human Rights. United Nations; 1948.

<sup>10</sup> International Covenant on Economic, Social and Cultural Rights. United Nations (General Assembly); 1966.

<sup>11</sup> International Covenant on Civil and Political Rights. United Nations (General Assembly); 1966.

<sup>12</sup> Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights. United Nations (Economic and Social Council); 1984.

# OBJECTIVES

The Principles are clustered around three interconnected objectives:

**(1) protect people – as individuals, as groups, and as communities**

**(2) promote health value – through data sharing and innovative uses of data**

**(3) prioritise equity – by ensuring equitable distribution of benefits that arise from the use of data in health systems**

Most current approaches to data governance take an individualistic view without also seeking to enact a solidarity-based approach that maximises the value of health data for

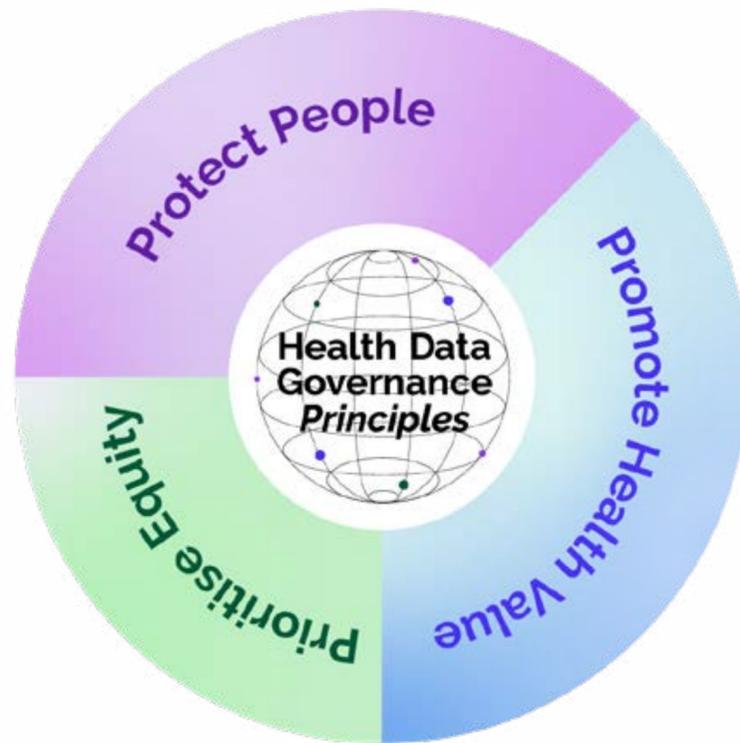
whole populations. The Health Data Governance Principles balance both individual and collective perspectives within each of the three objectives.

*Protect people* considers the importance of group and community data protections. *Promote health value* speaks to the collective needs and benefits of public health systems. *Prioritise equity* requires equity among groups and individuals.

The Principles are intended as a resource for, and have applicability to, a range of stakeholders involved in the governance of health data, including: governments, parliamentarians and policy-makers; international organisations, global health initiatives and development banks; the

private sector; non-profit and non-governmental organisations; research and academic institutions; donors and foundations; civil society (including activist groups, patient organisations, etc); global coalitions; data stewards and users; and the public themselves.

The Principles seek to unite stakeholders around core elements aimed at advancing equitable health data governance by creating a common vision and an environment where all people and communities can share, use and benefit from health data.



# DEVELOPMENT OF THE PRINCIPLES

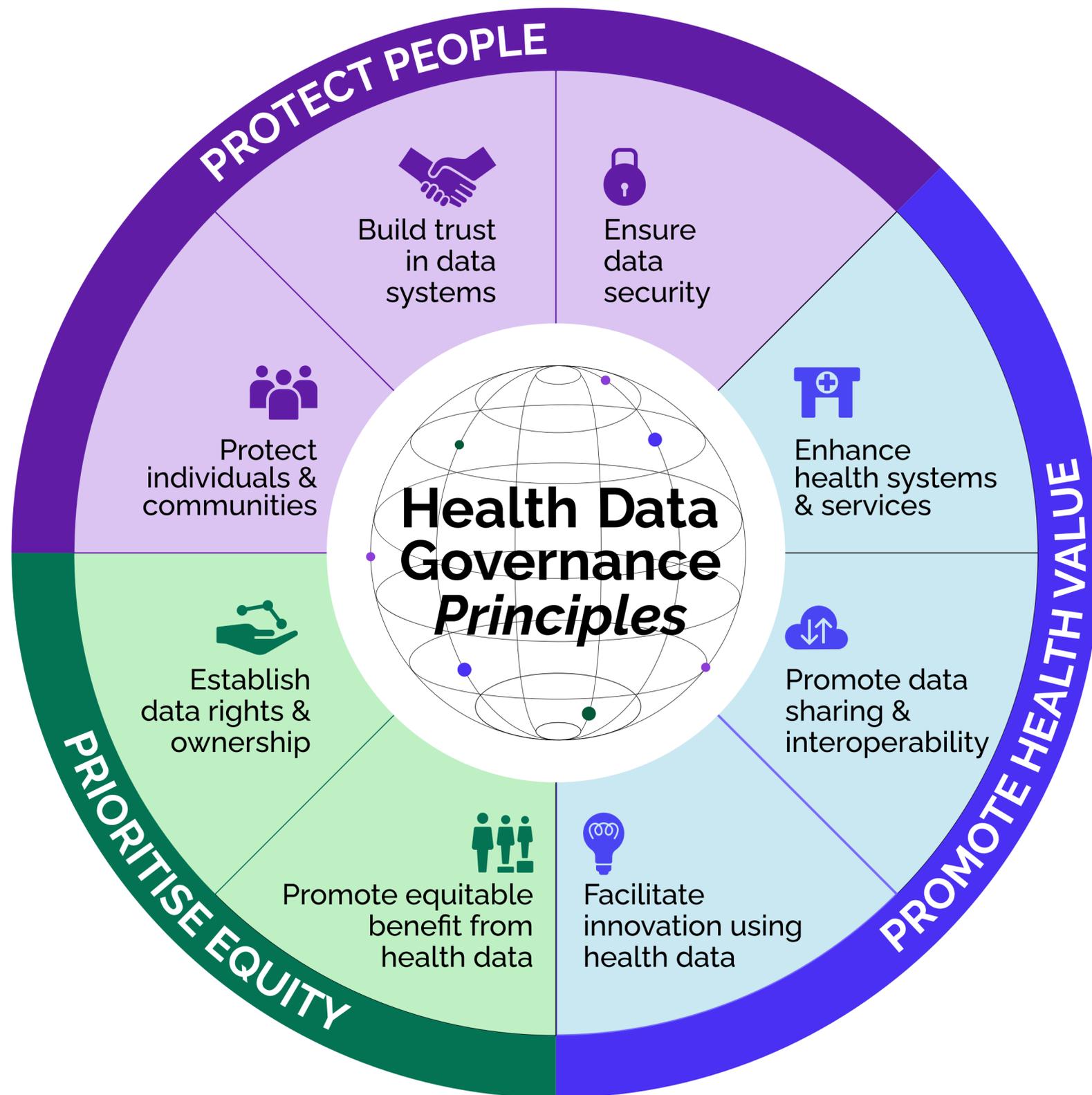
The Health Data Governance Principles have been primarily driven and developed by civil society through an inclusive and consultative, bottom-up process stewarded by Transform Health. This process brought together over 200 contributors from over 130 organisations through eight global and regional workshops covering Sub-Saharan Africa; the Middle East and North Africa; South, East, and Central Asia; Latin America and the Caribbean; and Europe, North America, and the Pacific. This was followed by a one-month public consultation on a draft

set of Principles. This process was designed to gather perspectives and expertise, and ensure meaningful engagement, of diverse stakeholders from across geographies and sectors.

Transform Health stewarded this process, under the leadership of its Policy Circle, which includes digital health and data governance experts from: Asia eHealth Information Network (AeHIN), FIND, Fondation Botnar, the Health Data Collaborative's Digital and Data Governance Working Group, I-DAIR, IT for Change, Jhpiego, PATH,

Philips Foundation / Digital Connected Care Coalition, Red Centroamericana de Informática en Salud (RECAINSA), and Young Experts: Tech 4 Health (YET4H). The following partners were instrumental in supporting the global and regional consultations: PATH, AeHIN, the BID Learning Network, Mwan Events, RECAINSA, Wilton Park, Governing Health Futures 2030 and YET4H. This work was funded by Fondation Botnar.





# THE 8 PRINCIPLES

The Health Data Governance Principles are designed to complement and reinforce one another. As such they are not weighted or listed in any order of priority. Each Principle is supported by core elements that further describe it and how it can be put into practice. The Principles are clustered around three overarching objectives: protect people, promote health value, and prioritise equity.

---

*Click on any Principle to be redirected to its description.*

# PROTECT PEOPLE

Health data governance must ensure protection for individuals, groups and communities against data-related harm and violations. Protection for individuals is often embodied in general data protection laws. However, due to its potentially sensitive nature, health data requires additional specialised protections in law and in data practices. Unprotected health data (personal and aggregate) could expose individuals, groups and communities to harm. Health data governance must include special measures of protection against various kinds of individual and collective harm, including data-driven exploitation, harassment, discrimination, surveillance capitalism and neocolonialism.

## PROTECT PEOPLE

# PROTECT INDIVIDUALS AND COMMUNITIES

Health data governance must protect individuals, groups and communities against harm and violations at every stage of the data lifecycle. Data governance should seek to balance the protection and rights of individuals, groups and communities with the societal value of data use for health. This balance requires rigorous evaluation and risk assessment of data practices to identify and mitigate potential harm, which should be built into every stage of the data lifecycle. Similarly, it requires meaningful participation of civil society, communities and individuals.



# Core Elements:

## **Address individual and collective risk**

Health data governance must prioritise the reduction of individual and collective risk, following the doctrine of “do no harm”. The collection and use of health data must mitigate potential risks individuals may face, which can range from moderate (e.g. loss of data privacy) to severe (e.g. risks to personal safety, risks of insufficient or incorrect care, exploitation). When data is not personally identifiable, health data governance should mitigate collective risks, including those related to a specific group or community (e.g. risks of discrimination) and those relating to the broader society (e.g. risks to public health).

## **Collect data with a defined purposes**

Specific data needs should be clearly defined prior to any data collection. Data collectors and stewards must communicate these needs to the individuals and communities providing their data. Health data governance must include guidelines on data collection needs and limitations (e.g. only collect data that is needed and use existing data where possible).

## **Collect personal or sensitive data only when necessary and with informed consent**

Personally identifiable or otherwise sensitive health data must be collected only when necessary to achieve a specific and justifiable health, research or policy objective (e.g. electronic health records may include sensitive data required to improve patient care). In this regard, health data governance policies, laws and regulations should follow global standards and best practices.

Data collectors and stewards must gather informed consent from individuals and communities before data is collected. Informed consent requires that individuals and communities fully understand their rights and how their health data may be used. When situations require exemptions to this requirement (e.g. public health emergencies), such exemptions must be legal, justified, and limited to the specific circumstance.



## **Use secure data collection and storage mechanisms**

Protection of health data requires secure methods of collecting data (e.g. using data collection tools with robust data protection functionality) and secure data storage (e.g. encryption, cloud servers). Consideration should be given to how long data is stored, with guidance on a reasonable timeframe after which data should be deleted or otherwise removed from the system (e.g. sunset clauses). Because personal health data is “lifetime” data, the data retention policies related to care records should not create gaps in longitudinal health records. Comprehensive data security policies should also respond to data transfer approaches (e.g. USB drives, external hard drives, routers, servers, databases) and the evolving health innovation ecosystem.

## **Use de-identification and anonymisation**

Health data governance should define the level and the extent of privacy protection to which an individual is entitled, and the associated mechanisms to ensure such protection. For every stage of the data lifecycle,

health data governance must indicate where de-identification and anonymisation is necessary for individual and community protection. In addition, health data governance should outline protections for de-identified and anonymised data, as even this data may expose sensitive information. The possibility of re-identification resulting from rapid technological developments should also be considered (e.g. by data analysis algorithms or triangulation of data sources).

## **Define inappropriate uses of health data**

Health data governance should specifically address unlawful, inappropriate and unethical collection or use of health data. This may include non-health-related surveillance by state or other actors or discrimination and harassment by public or private stakeholders, especially against marginalised groups and populations. National and global governance frameworks, relevant to the digital age are necessary to uphold fundamental human rights while collecting, processing, storing, analysing, using, sharing and disposing health data.



## **Institute safeguards against discrimination, stigma, harassment and bias**

Health data governance must institute and strengthen approaches and processes to address and prevent social discrimination, stigma, harassment and bias, as a necessary component of health system design and regular audits. Health data governance must consider the cultural context to which it is applied. Training and empowering health workers and meaningfully engaging diverse communities will be important to help mitigate discrimination, stigma, harassment and bias.

## **Provide guidance specific to marginalised groups and populations**

Health data governance practices must be aware of and responsive to the unique contexts and data-related needs, as well as possible data-related harms,

of marginalised groups and populations. Practices that may seem harmless to the general population may carry specific data-related dangers to certain groups and communities, such as groups at higher risk for HIV (e.g. sex workers, injecting drug users, informal workers, transgender people).

Relevant guidelines should assert the importance not only of recognising the unique contexts of vulnerable populations, but also of the meaningful inclusion of such groups when formulating governance principles more generally. Existing recommendations and other guidance specific to marginalised groups and populations should be incorporated into health data governance policies and processes. For example, UNICEF has produced a [manifesto on the better governance of children's data](#)<sup>13</sup>.

---

<sup>13</sup> The Case for Better Governance of Children's Data: A Manifesto. NY: UNICEF; 2021 (<https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf>, accessed 3 December 2021).



## PROTECT PEOPLE

# BUILD TRUST IN DATA SYSTEMS

Well-developed health data governance should reinforce trust in data systems and practices. Developing health data governance systems in a participatory and transparent manner, and ensuring regulations and guidelines are accessible, understood, and followed in practice, can help build trust. Trust requires safeguarding data, preserving privacy, and establishing transparent and inclusive data collection, processing, storage, analysis, use, sharing and disposal processes. It also requires responsiveness to questions from data subjects and other stakeholders and mechanisms to address grievances.



# Core Elements:

## Align with best practices for data protection and privacy

Health data governance should apply existing—and establish new—best practices to protect individual and collective data. This includes both technical approaches to data collection and storage (e.g. two-factor authentication, encryption, de-identification) and policies and processes related to how data is accessed and used (e.g. security policies, system permissions). Health data governance should align with, and learn from, well-established policies and regulations, such as the [General Data Protection Regulation \(GDPR\) in Europe<sup>14</sup>](#), the [Personal Data Protection Act \(PDPA\) in Singapore<sup>15</sup>](#), and the [Protection of Personal Information Act \(POPI Act\) in South Africa<sup>16</sup>](#).

## Ensure consent is informed and understood in all its complexities

When collecting an individual's data, the data subject has a right to understand what data is collected, why it is collected, and their rights regarding accessing, changing or removing their data from the system.

Individuals should clearly understand how their data inform personal care and whether their data may be reused for additional purposes. Individuals should also have a reasonable option to accept or decline data collection as appropriate, as well as the option to accept or decline further sharing of their data for purposes other than its initial intended use. Individuals must also be able to withdraw their consent. Informed consent must be articulated clearly (including in the local language) to ensure accessibility to those unfamiliar with technical or legal language.

Informed consent is the gold standard for health data governance. However, health data governance policies and processes must acknowledge the complex reality of informed consent, particularly for marginalised groups and populations. For example, an individual may be required to provide their data to receive health services, and so may feel compelled to consent regardless of their understanding of or agreement with how their data may be used. In all instances,

<sup>14</sup> General Data Protection Regulation (GDPR). 2018 (<https://gdpr-info.eu>, accessed 5 May 2021).

<sup>15</sup> Personal Data Protection Act (PDPA). 2012 (<https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act>, accessed 5 May 2021).

<sup>16</sup> Protection of Personal Information Act (POPI Act). 2019 (<https://popia.co.za>, accessed 5 May 2021).



the protection and informed agency of an individual or community should be the highest consideration. Health data governance should therefore articulate a nuanced view of consent considering the circumstances, the range of realistic options, and the power relationships in a given situation.

### **Obtain collective consent where appropriate**

Health data may be related to a specific community or group characteristic (e.g. patients with a rare disease, groups vulnerable to a specific disease). In such cases, collective consent may be necessary. This both upholds collective rights and serves to build and maintain trust.

### **Define concrete exceptions to informed consent**

Health data governance policies and processes should clearly and transparently define circumstances where exceptions to informed consent are permitted. Exceptions should be limited to instances where life-saving interventions require a proxy; where individual consent requirements pose an acute barrier to public health (e.g. during public health emergencies); where

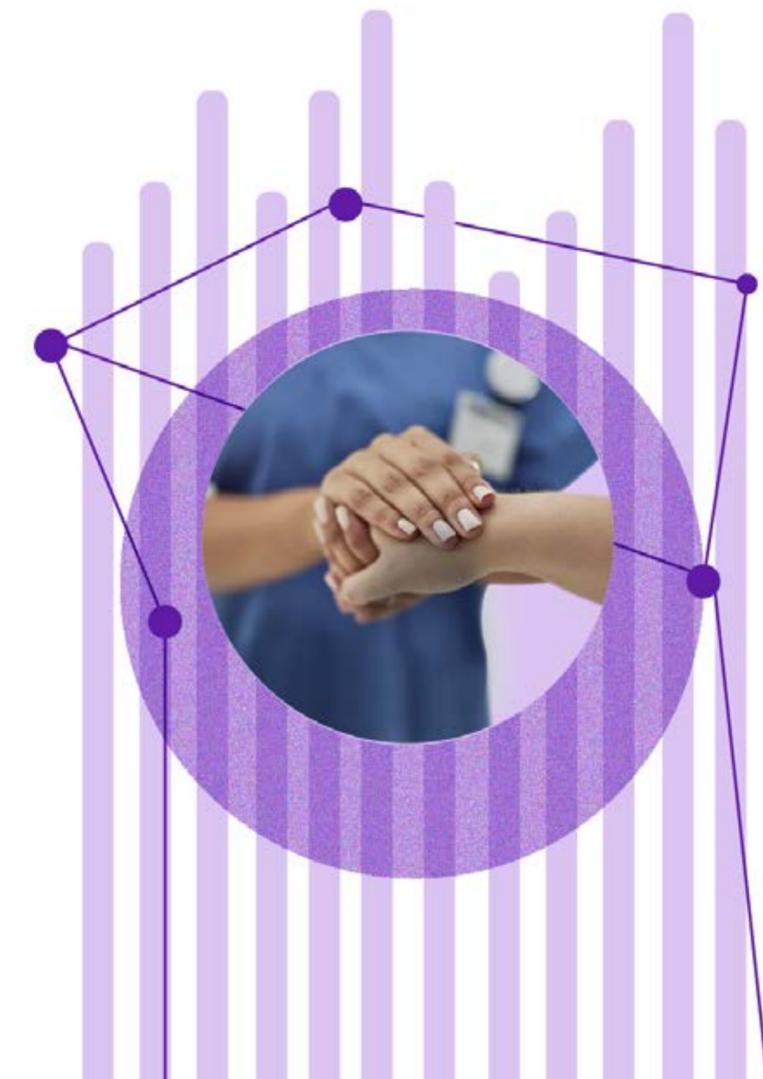
there is a legitimate and justifiable legal requirement; or where data is processed or shared in aggregate form (e.g. population-level data). Exceptions to informed consent should be legal, necessary, and proportionate, and must not be misused to harm or exploit an individual, group or community.

### **Ensure data quality, availability, and accessibility**

Trust in data systems also requires trust in the quality of data. Health data governance should advance overall improvement in data quality and make data more available and accessible, as appropriate. Global standards must be adopted and adapted to regional, national and local contexts to promote high-quality, accurate and reliable data collection.

### **Reinforce health data governance with evidence**

Health data governance should be informed with evidence from its use and impact, both positive and negative. It should also be regularly evaluated against best practices. When gaps in existing practices and/or knowledge are identified, efforts should be made to address these gaps and contribute to the global



evidence base regarding health data governance. This includes regular interactions and learning across global and national digital health frameworks. These efforts should contribute to the continued evolution of health data governance.

### **Establish transparent and accessible processes and systems**

Transparency in health data governance can create buy-in from stakeholders around data processes, thus enabling better re-use of data, greater collaboration on data analysis methodologies, and higher-quality insights from data. The [Data Futures Partnership](#)<sup>17</sup> in New Zealand defines transparent data use with three dimensions: value, protection, and choice. All stakeholders involved should understand how and why data are collected (value); how data are stored, analysed, and used (protection); and how the systems and processes that support health data governance operate (choice).

Transparency is essential to both public and private sectors. While public policies on data, artificial intelligence, and emerging technologies must be open, participative and people-centric, private sector services, such as telemedicine, must build trust with patients by acknowledging local contexts, languages and values.

### **Institute feedback and accountability mechanisms**

Inclusive, equitable and accountable health data governance requires mechanisms through which individuals and communities can report data misuse, make inquiries into health data structures and processes, remove their data from a system, and provide general feedback. These processes must be supported by mechanisms like statutory data auditing and independent oversight. Individuals and communities must be proactively informed of their right to feedback and of such processes and mechanisms. Data contributors should also be kept informed of, and receive benefits that arise from data sharing and data usage.

<sup>17</sup> Data Futures Partnership. Government of New Zealand; 2015 (<https://www.stats.govt.nz/assets/Uploads/Retirement-of-archive-website-project-files/Corporate/Cabinet-paper-A-New-Zealand-Data-Futures-Partnership/nzdf-partnership-overview.pdf>, accessed 3 December 2021).



## PROTECT PEOPLE

# ENSURE DATA SECURITY

Data security is an essential component of health data governance, encapsulating technical and procedural requirements for the protection of individuals and communities. This includes applying best practices for the collection, processing, storage, analysis, use, sharing and disposal of health data. This Principle is relevant beyond the health sector, and security-related best practices must continually evolve as new technologies are introduced.



# Core Elements:



## **Require strong technical security measures for data processing**

Any technical processes employed to collect, process, store, use or share data should employ robust security mechanisms, for which threshold guidelines need to be defined. This may include password requirements, two-factor authentication, security keys, and data encryption. Data storage and processing facilities must be secured as per global or national standards. In addition, health data governance should address common security risks, including phishing and viruses. Data security must be instituted right from the design of technologies and processes to foster trust. Data security audits should be undertaken periodically.

## **Mitigate risks related to security threats**

Health data governance should consider how to minimise the impact of potential security breaches on individuals, communities and health systems. This may include using unique identifiers in place of an individual's name; placing limits on how long data

may be stored; adding enhanced security measures for personally identifiable or otherwise sensitive data; reassurance initiatives on cybersecurity; safe storage guidelines for confidential data; and efforts to respect, protect and uphold the right to privacy as a system design principle.

## **Ensure transparency around data breaches**

When data breaches do occur, health data governance should require stakeholders to inform the individuals and communities affected and report the breach to the concerned regulators. Information should be provided on the nature of the breach, what data may have been exposed, and specific actions that were taken to prevent a similar breach in the future. Every significant breach must be reviewed by independent oversight mechanisms.

### **Consider federated data systems**

Data security, data rights, and data ownership may be enhanced through federated storage, processing and use of data. Federated data systems allow data to remain close to their point of generation (e.g. at the health facility concerned) while still allowing consent-based viewing and analysis across the health system.

They bring together multiple, autonomous data sources to allow cross-system sharing and learning while appropriately adapting good data practices across different sectors. This approach may maximise the value and use of data and create new opportunities to generate insights from multiple stakeholders across sectors.



# PROMOTE HEALTH VALUE

Health data governance must maximise the value obtained from the use and analysis of data to improve health outcomes for both individuals and society. Often, this requires some forms of data to be shared widely as data silos can lead to under-optimal creation of health value. The aggregating and sharing of health data must be done in a manner that protects individual, group and community rights. Further, as data-based approaches can lead to new kinds of health services, health data governance must support and promote such innovations.

## PROMOTE HEALTH VALUE

# ENHANCE HEALTH SYSTEMS AND SERVICES

Health data governance should enable the meaningful use of data to enhance health system efficiency and resilience, improve health access, and advance health equity, towards achieving Universal Health Coverage. A whole health system approach must be applied, ensuring health data governance supports the systemic transformation of health systems. The benefits of well-governed health data should be fully inclusive of individuals and communities who contribute their data.



# Core Elements:

## Evaluate the benefits of health data

In addition to improved access to health services, health data offers opportunities for greater quality, efficiency, effectiveness, and sustainability of health systems. Data use also creates opportunities for innovation and advancements in medical sciences. The value offered by these advancements should be considered when defining the potential use of health data. For example, data may be needed by research institutions and academia for research and development purposes. These stakeholders may legitimately require appropriate, secure access to data, but individuals and communities who contribute data must also fully understand how their data may contribute to research and development.

## Use data to enhance health services for individuals and communities

Health data governance must enhance the use of health data for better health and well-being, including of individuals and communities who provide their health data. This can be accomplished in various ways (e.g. improved access to health services,

robust surveillance, better diagnostics and predictive analysis, precision medicine). Improving individual care and ensuring patient safety requires data sharing between health facilities and health providers to support a continuum of care. Data sharing is also needed to support public health informatics and data-led actions. Data sharing and access policies should be designed to enable such use of data.

## Encourage a culture of data-led insights and action

Health data adds significant value to health systems and services, leading to personal and public health improvements. Health data governance should encourage a culture of exploring, developing and using data insights at all levels of a health system to address health inequities and improve health services. Health data governance should be designed in such a way to build confidence in data users and decision-makers, not only that the data used is of high quality but also that the data is legally and ethically obtained and managed.



### **Address health system efficiency, effectiveness, and resilience**

Appropriate health data governance is a prerequisite to a resilient and responsive health system and can improve the efficiency and effectiveness of health services. These benefits can extend to all operational components of a health system (e.g. supply chain, health workforce management). Health data governance should include operational improvement when defining data needs.

### **Strengthen community ownership of health data**

Centralised data systems centralise decision-making and power. Health data systems should be designed and operated in a manner that increases rather than decreases community-level autonomy, management, and decision making related to the collection and use of health data.

### **Enable and empower frontline health workers**

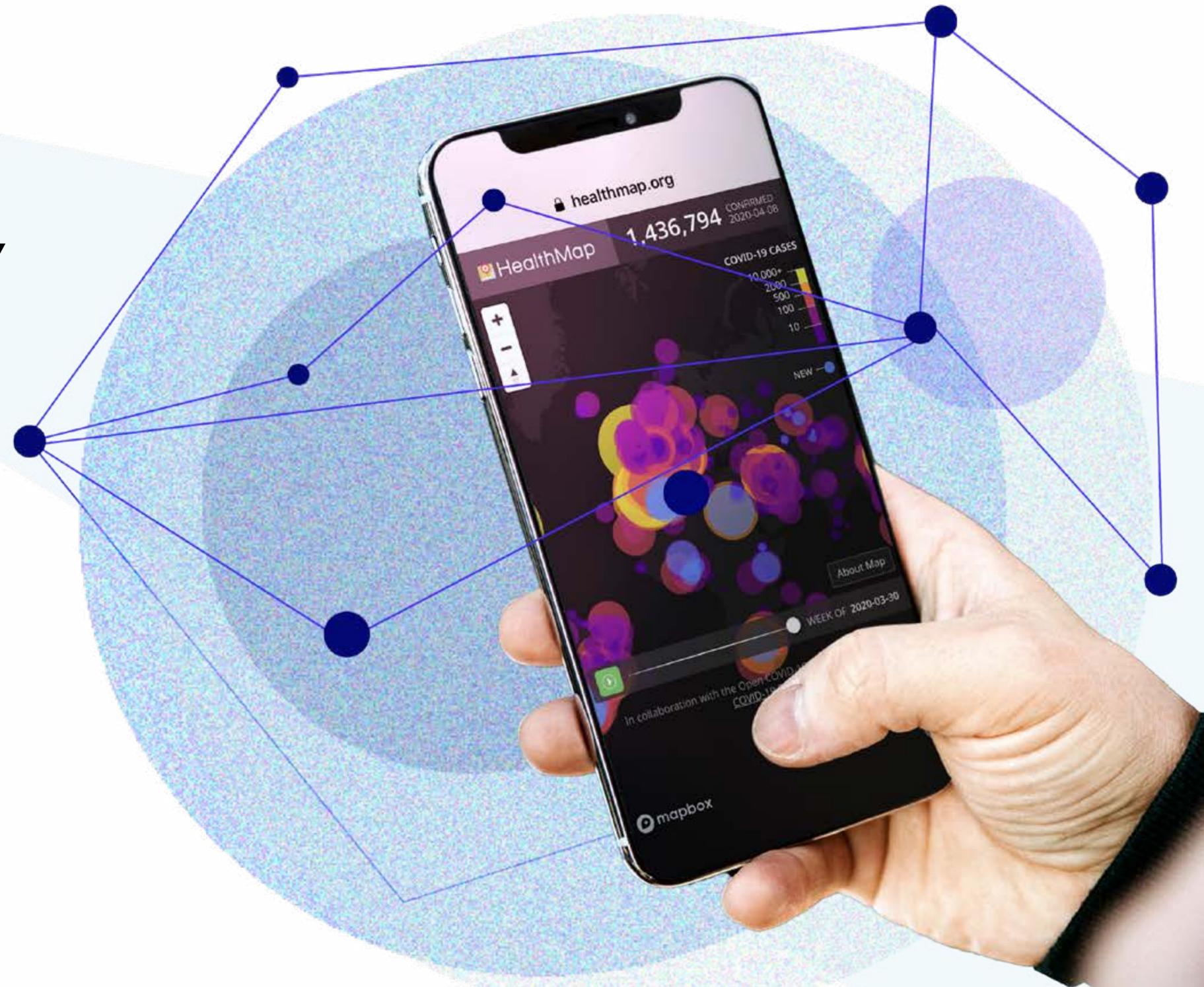
Health data governance should address and enable the critical role, value and agency of frontline health workers, which should be central in the design of data-based health systems. There must be an intentional effort to ensure that data-based decision-making does not weaken the role of frontline health workers as a mere extension of centralised systems, but rather that their role is strengthened through their use of data-based insights in their daily work. Frontline health workers should be offered continual skill building along with other resources to support their collection and use of health data. Frontline health workers should also be engaged in the design, development and continual improvement of data (based) systems.



## PROMOTE HEALTH VALUE

# PROMOTE DATA SHARING AND INTEROPERABILITY

Data sharing is a prerequisite for creating value from health data but must be done in ways that support equity and human rights. At national, regional and global levels, data sharing allows for deeper and more significant insights related to health needs and challenges, including preventing and responding to health emergencies. Systems designed for interoperability, e.g. around common protocols, structures and definitions, enable continual sharing of data, as well as ensuring data quality.



# Core Elements:

## **Establish data sharing rules and guidelines**

Health data governance should include data sharing rules and guidelines that address a range of data sharing scenarios. This includes data sharing required for individual care delivery, among public agencies within a country, between government systems and the private sector, within the private sector, and between national, regional and global stakeholders. International data sharing and transfer may require additional global standards to align differing national systems and frameworks.

Data sharing policies should minimise both individual and collective risk even as they enhance public health equity. Leveraging data sharing to use previously collected data can even reduce the need and extent of new data collection.

## **Validate informed consent before sharing data**

Data should only be used for the purpose for which it was collected unless informed consent for subsequent uses has been obtained from the individual or, if relevant, group or community. If clear data-sharing agreements are not in place before data collection,

additional consent may be required from individuals, groups or communities who originally contributed data.

## **Promote interoperability of data systems**

Data, and the digital health systems that support their collection and use, should be designed with interoperability in mind. Interoperability will make sharing data between systems simpler and more secure while preventing potential errors during manual data transfers. Interoperability is accomplished through the application of recognised standards (e.g. basic data fields) and system design (e.g. use of open Application Programming Interfaces/APIs). Concepts like data portability, open data, community data, data trustees, and data exchanges may also be considered as part of the sharing and interoperability mechanism.

## **Define common data structures across health systems**

Common data structures (e.g. specific fields for data collection, the underlying architecture of data systems) will support data sharing as well as the use of emerging technologies by allowing predictability and easier consolidation of data from a variety of



data systems. Such common structures enable interoperability and opportunities for deeper and more complex insights that add value and efficiency to medical sciences and improve health outcomes. Such common structures also provide assurance as to the types of data available for future use.

### **Define multiple levels of data access**

Health data governance should outline limitations on data access, identifying which stakeholders will have access to various levels of data, including de-identified or anonymised data. This should balance the need to minimise risk of exposure with maximising sharing that can lead to additional value. These permissions may exist on a technical level (e.g. systems permissions) and/or arranged through institutions like data trusts, that clearly define rights, roles and responsibilities of different actors.

### **Use common definitions and global standards**

Health data governance should utilise existing terminology and definitions of key concepts like data

types, system protocols, and stakeholder roles and responsibilities. Such definitions are provided by global normative bodies, and are widely used in both the public and private sectors. Existing data standards and frameworks (including [ISO/TS 22220:2011<sup>18</sup>](#), [HL7 FHIR<sup>19</sup>](#), [OpenHIE<sup>20</sup>](#), [GS1<sup>21</sup>](#), and others) should be applied whenever possible. This promotes greater standardisation and comparability of health data, which allows for greater systems interoperability, data sharing, data quality, and data hygiene.

### **Support multi-sector partnerships**

Health data governance should support partnerships between national governments, the private sector, academic institutions, civil society, non-governmental organisations, and other types of stakeholders, to create a safe, robust, and resilient ecosystem of data collection, processing, storage, analysis, use, sharing and disposal. Clear policies are needed to build trust and partnerships among stakeholders. These policies should prioritise the interests of individuals and communities that provide data and larger societal interests, especially of public health equity.



<sup>18</sup> ISO/TS 22220:2011: Health informatics — Identification of subjects of health care (<https://www.iso.org/standard/59755.html>, accessed 20 September 2021).

<sup>19</sup> HL7 Fast Healthcare Interoperability Resources (FHIR) (<http://hl7.org/fhir>, accessed 20 September 2021).

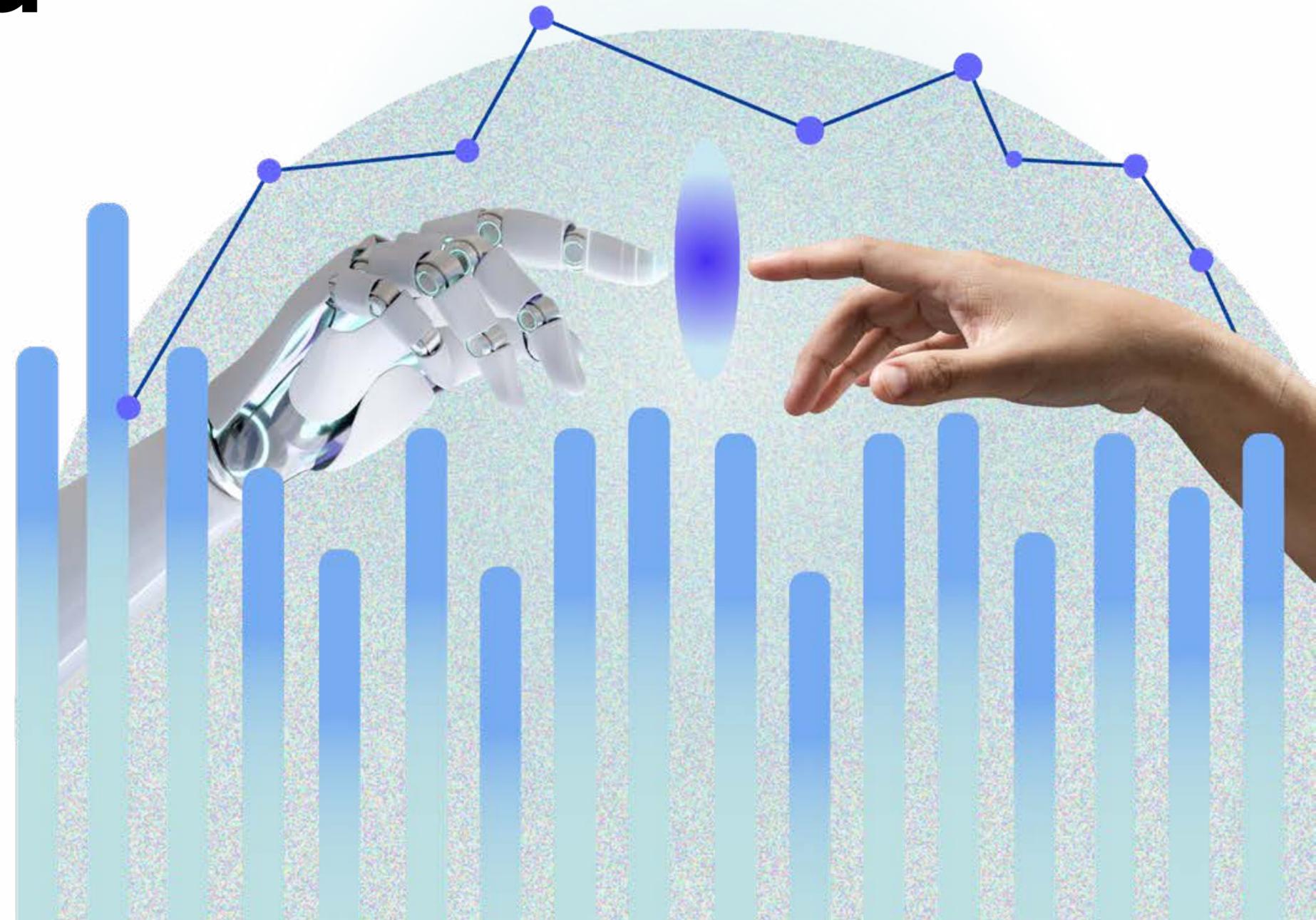
<sup>20</sup> OpenHIE (<https://ohie.org>, accessed 20 September 2021).

<sup>21</sup> GS1 (<https://www.gs1.org>, accessed 20 September 2021).

## PROMOTE HEALTH VALUE

# FACILITATE INNOVATION USING HEALTH DATA

Health data governance should be forward-looking and anticipate (wherever possible) the application of emerging technologies, such as artificial intelligence (AI). Leveraging the continual evolution of digital technologies and data systems is key to achieving the Sustainable Development Goals and UHC. This requires developing a governance environment that can flexibly accommodate and enable innovation and be effectively applied to new digital technologies and new kinds of data uses.



# Core Elements:

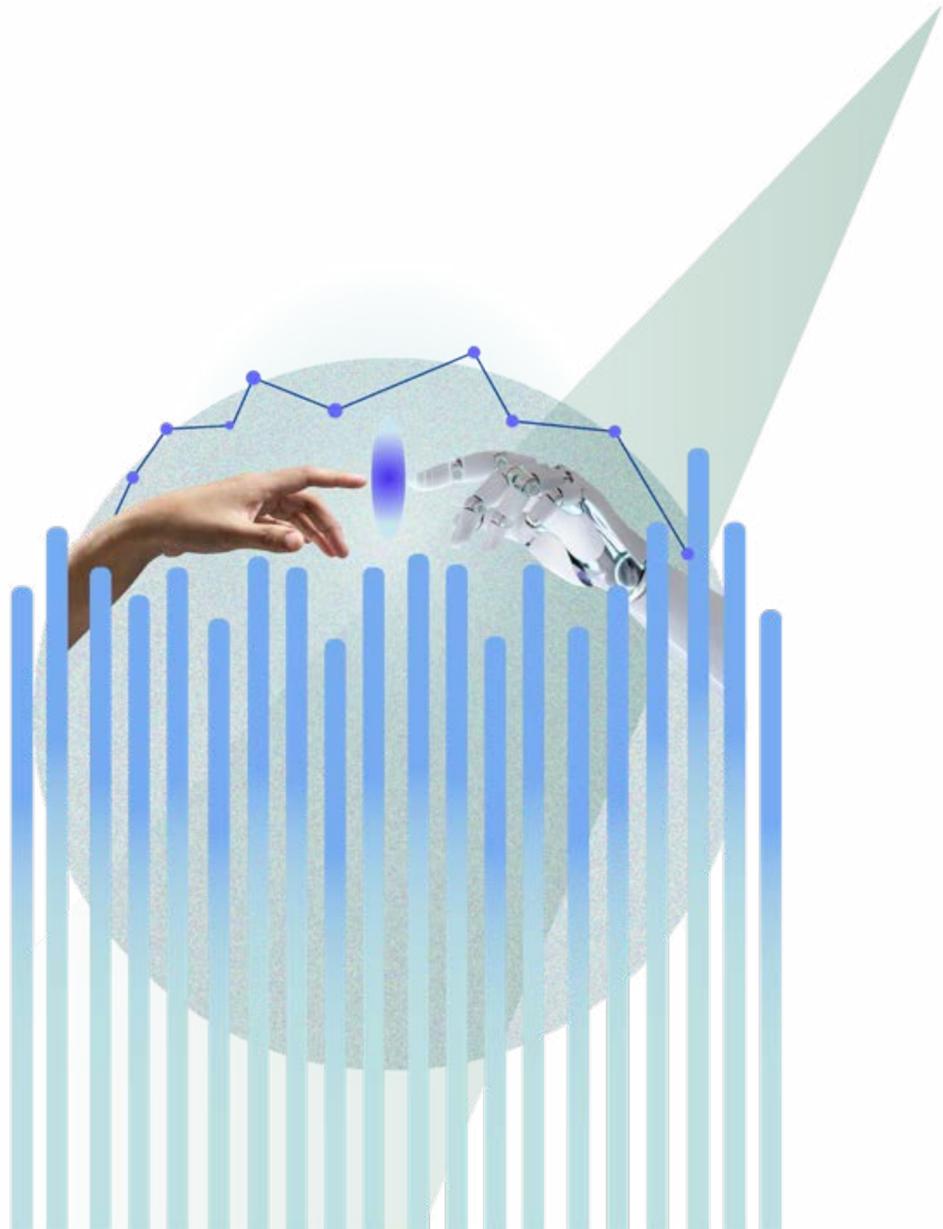
## Apply health data governance to emerging technologies

Emerging technologies cannot be exempt from checks and constraints instituted by health data governance. New and emerging digital technologies should consider health data governance principles, policies, and legislation from the ideation and design stages. Mechanisms should be defined to address potential conflicts between existing health data governance and the needs of emerging technologies. Sandbox facilities for controlled testing of technical and business innovations may be useful in this regard. In the face of rapid technological development, more general guidelines may be needed in addition to specific rules that address current and known technological contexts, such as [WHO's Guidance on Ethics and Governance of Artificial Intelligence for Health<sup>22</sup>](#).

## Address the use of non-health data in health contexts

Many digital health technologies and practices utilise data from sources beyond health systems. Health data governance should consider other types and sources of data that may be combined with health data. When combining health data with data from other sources, the intended use of data must be clearly defined and uphold the principles of health data governance (e.g. promoting health equity and protecting the individual). Combining data from multiple sources may create additional risks to the individual (e.g. re-identification), which must be mitigated. This will require a flexible understanding of what data falls under the remit of health data governance. However, such data may also offer new and more impactful opportunities for health systems. Health data governance should therefore not become unduly restrictive as related to new data types and categories.

<sup>22</sup> Ethics and governance of artificial intelligence for health: WHO guidance. Geneva: WHO; 2021 (<https://www.who.int/publications/i/item/9789240029200>, accessed 5 May 2021)



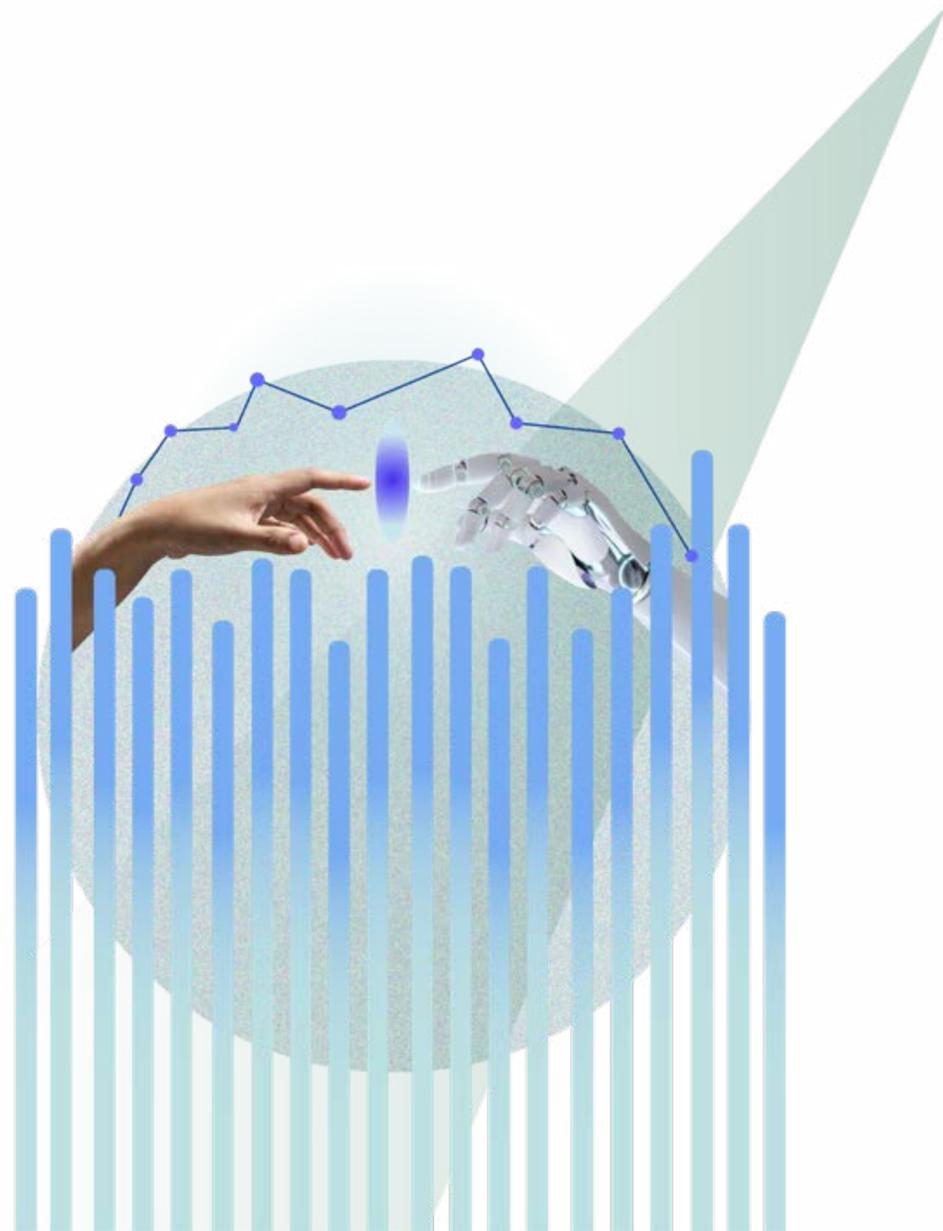
### **Build public health data infrastructure**

The development and strengthening of digital public infrastructure (including data) will facilitate health service delivery and innovation. Such health data infrastructure would gather real time data from many sources and make it available in a safe and ongoing manner to health service providers and innovators. Digital public infrastructure could serve as a proactive and flexible mechanism for technical and process innovations.

### **Employ policy innovation**

Policy and legislation may lag behind the technological capacities of data collection, processing and use, including the emergence of new digital technologies and creation of new business models. New policies—and new types of policies—may be needed. Broader policy frameworks that cover a range of possible and emergent scenarios, sandbox facilities, and temporary, informal use of emergent standards

or practices are examples of policy innovation. Such policy innovations must guide the use of emerging technologies towards appropriate use of health data, and not otherwise. While new policy approaches may be needed to support innovation (e.g. the development of precision medicine or the application of big data for developing new medical devices), they cannot lose sight of the key objective of guiding data-based innovations towards health equity and ensuring UHC.



# PRIORITISE EQUITY

Health value created by the use of data must equitably benefit individuals and communities. Data is contributed by people, whether as individuals or as communities, and so people should have an equitable stake in the health value that their data generates.

## PRIORITISE EQUITY

# PROMOTE EQUITABLE BENEFITS FROM HEALTH DATA

Equity must be inherent to health data governance—ensuring equitable representation in data of all individuals, groups and communities, regardless of social or economic characteristics, as well as equitable access to data-generated health value. Equitable health data governance reinforces population-sensitive applications of health data in health services and systems. It also promotes the equitable sharing of data-led health service improvements and innovation, especially with the data contributing individuals and communities. Equity in health data governance must extend beyond policies, processes and outcomes to include public engagement, education and meaningful participation of all groups in relevant decision-making about health data systems.



# Core Elements:

## **Represent all groups and populations equitably in data**

Health data should be inclusive and equitably representative of all groups and populations, regardless of demographic or social attributes (e.g. age, sex, gender identity, race, ethnicity, citizenship status, refugee status, sexual identity, ability) or economic characteristics (e.g. education level, income status, profession). This requires inclusive data collection methodologies and processes that consider which individuals, groups or communities are asked to provide data; which data categories are collected; and what is the intended use of collected data.

## **Consider the unique needs of marginalised groups and populations**

In order to equitably consider the unique needs of marginalised groups and populations related to health data governance, the collection and analysis of data must be intersectional and cross-cutting along categories like gender, sex, sexuality, age, socio-economic status, abilities, citizenship status, class, race, and ethnicity.

Health data governance must also address unique protection needs of marginalised groups and populations. For example, exposing information on sexual and gender identity can place individuals at risk of arrest or violence in some contexts. Marginalised groups must be actively and meaningfully involved in the development, implementation and review of health data governance policies and practices.

## **Mitigate data bias**

Bias may be introduced at any point in the collection, processing, and use of data. Such bias can perpetuate inequities, undermine the integrity of data, and can lead to incorrect or incomplete insights. Bias also leads to discrimination and exclusion, whether intended or not. Health data governance should aim to identify where bias may be introduced and counteract its effects. It must provide mechanisms to report and address existing biases within data systems and protect against continued misuse of health data that reinforces bias.



### **Use accessible language and plug knowledge gaps**

Health data governance should be understandable to the general public and written in gender-neutral language. It should be accessible to children, individuals with low literacy, and those who speak minority languages. While specific legal or technical documents may be needed to legislate or operate health data governance, supporting resources should enhance individuals' and communities' understanding of their rights in a practical, actionable way. Efforts should be made to enhance the general public's knowledge of health data governance and how it may impact them on an individual, community and societal level.

### **Implement inclusive data feedback mechanisms**

Feedback mechanisms should be established so that individuals, communities, and institutions that serve them, are aware of how data is used at every stage of the data lifecycle. Individuals and communities who provide their data, and individuals involved in the collection of health data (e.g. frontline health workers)

should understand the purpose and outcomes of data use. Individuals and communities must also have agency over their data and be capable of making appropriate decisions for themselves. Ensuring this will support meaningful civil society and community engagement during data collection and beyond.

### **Promote equitable impact and benefit**

Health data governance should ensure that the benefit of data use and data-based health systems is equitably shared across all groups and populations, regardless of social, economic or political characteristics. This may entail improving the design, reach and accessibility of data-based systems to be inclusive of the needs of diverse groups and populations. Benefits gained from data must be shared fairly and equitably with individuals and communities who contribute data. In addition, proactive measures are needed to ensure that data use and data-based systems specifically aim at providing equitable and high-quality health services for marginalised groups and populations.



**PRIORITISE EQUITY**

# ESTABLISH DATA RIGHTS AND OWNERSHIP

Health data governance should be rooted in strong and clear data-related rights. Data-related norms, principles, policies, and laws should be drawn from such overarching rights. This includes consideration of all human rights, including the right to protection and safety, and the right to benefit equitably from data contributed, both at individual and community levels. Data ownership implies that individuals and communities have a right to know, determine, and control how their data are used, and to benefit equitably from such data. Such rights extend to products and services derived from data, such as AI. Health data systems, and their governance, should be designed based on such data rights and ownership.



# Core Elements:

## Apply a human rights lens to health data governance

Human rights — as expressed in documents such as the [Universal Declaration of Human Rights](#)<sup>23</sup>, the [International Covenant on Civil and Political Rights](#)<sup>24</sup>, and the [International Covenant on Economic, Social, and Cultural Rights](#)<sup>25</sup> — must be central to the articulation of data rights and ownership. Many rights, including both traditional rights (e.g. security, health) and new rights associated with data (e.g. privacy) apply to multiple data use scenarios. For example, rights related to women's or workers' safety could be applicable in a given data use context or process. The individual and collective rights of marginalised groups and populations should be given particular consideration.

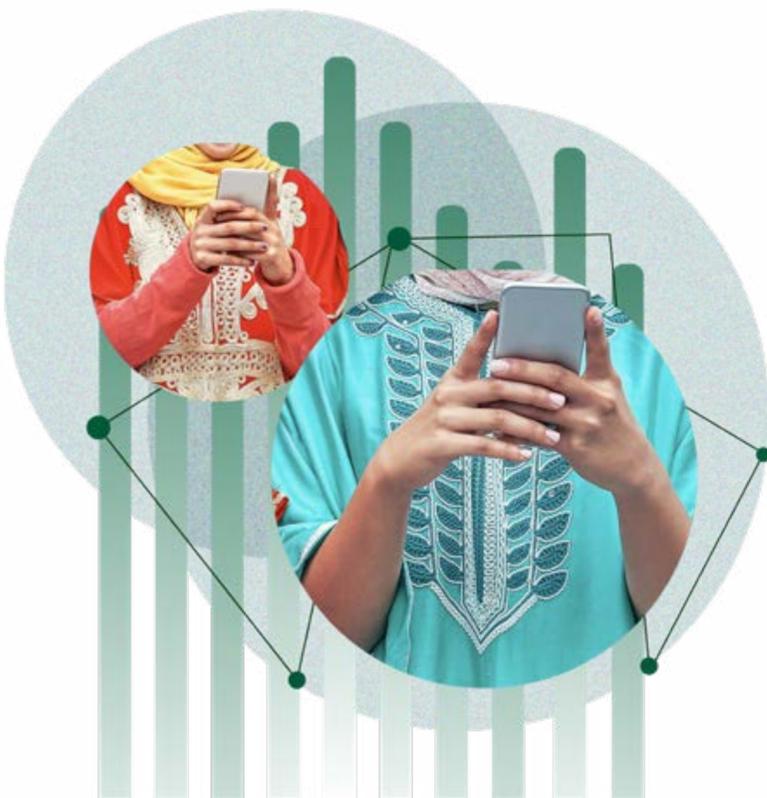
## Define clear governance roles and responsibilities

To ensure rights and ownership, it is important to clearly define various relevant roles within health data

systems, including data owner, data custodian, data processor, data steward, data trustee and data use beneficiary. Such roles should clarify who has what rights and who must ensure that these rights are upheld. These roles should include clearly defined responsibilities, particularly related to data privacy and protection, and benefit-sharing. The definitions used in existing data governance guidelines such as [GDPR](#)<sup>26</sup> and [PDPA](#)<sup>27</sup>, and other emerging frameworks, can be adapted or used in this regard.

## Codify data rights and ownership

Data rights and ownership should be codified in legislation and policy in alignment with current and emerging national, regional, and global norms, policies, laws and regulations. This should include definitions of ownership (e.g. health data is owned by the individual or community providing the data) and related rights (e.g. the right to control the use of data, the right to decline participation in data collection, the right to withdraw data from a system,



<sup>23</sup> Universal Declaration of Human Rights. United Nations; 1948.

<sup>24</sup> International Covenant on Civil and Political Rights. United Nations (General Assembly); 1966.

<sup>25</sup> International Covenant on Economic, Social and Cultural Rights. United Nations (General Assembly); 1966.

<sup>26</sup> General Data Protection Regulation (GDPR). 2018 (<https://gdpr-info.eu>, accessed 5 May 2021).

<sup>27</sup> Personal Data Protection Act (PDPA). 2012 (<https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act>, accessed 5 May 2021).

the right to obtain benefit). Further, the right to access data can be different from owning that data. These definitions should be linked with the defined roles and responsibilities of health data stakeholders. Health data governance should outline and provide the mechanisms for exercising such rights and ownership.

### **Extend data rights and ownership to products and services**

Data rights and ownership extend beyond data to related products and services, such as AI. Because data should not be used to harm individuals or communities, the products and services derived from such data should also not be used to cause harm. Similarly, individual and community ownership over their data extends to the right to equitable benefit-sharing from the products and services built from their data.

### **Develop health data trusts and health data cooperatives**

For effective implementation of health data rights and ownership, as well as widespread sharing of data, health data trusts and health data cooperatives should be developed. Such institutions define rules of data collection, processing, storage, analysis, use, sharing and disposal in a manner that respects the data rights and ownership of individuals and communities, while also actively providing them the means to exercise their data rights and ownership. Data trusts and data cooperatives are also an appropriate means for safely sharing data across the broader health landscape. They may be run by neutral third parties or representatives of data subjects.



### **Employ participatory data governance mechanisms**

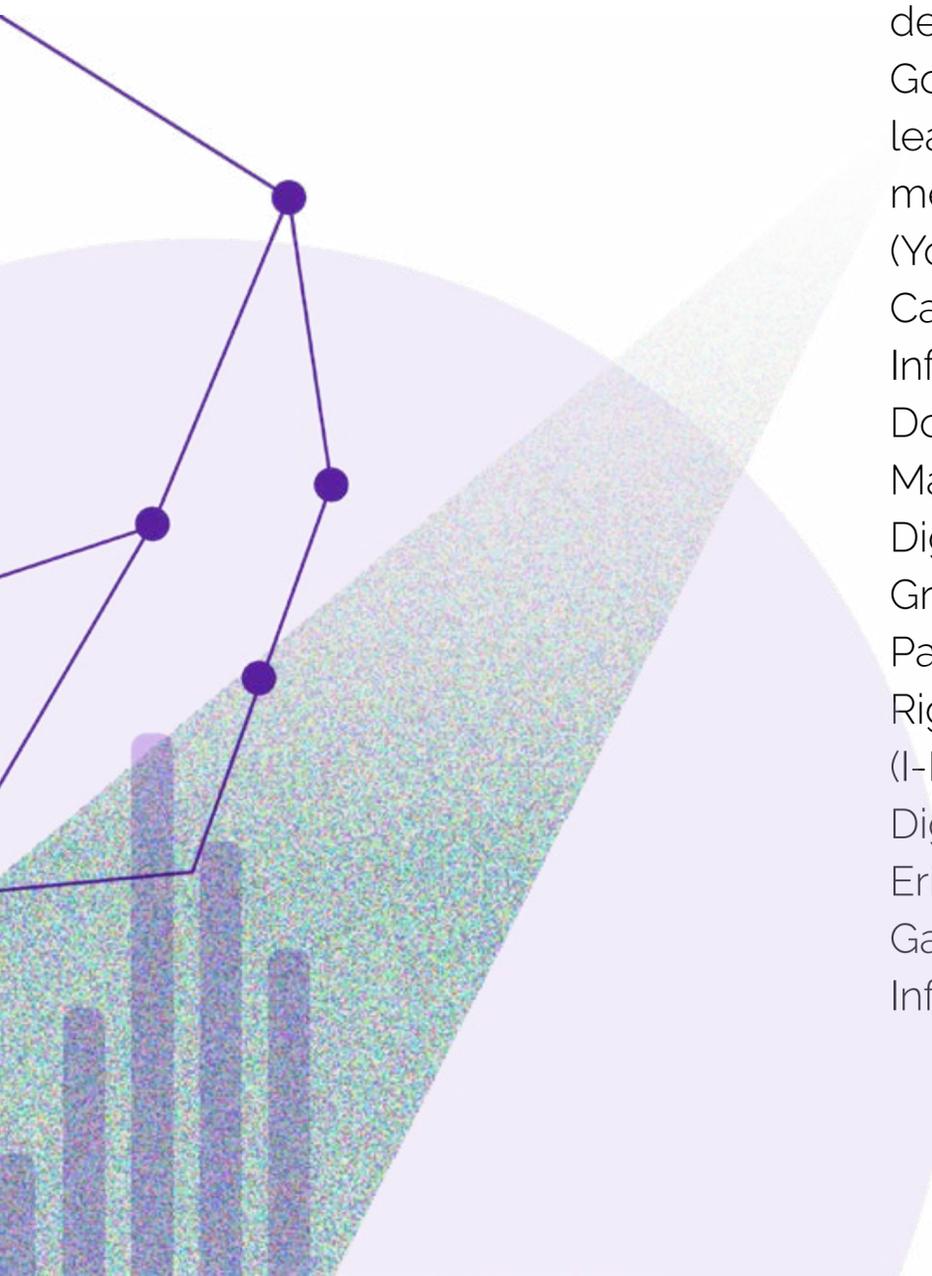
Data governance norms, principles, policies, rules and practices must be developed in an open and fully participatory manner. This could include mechanisms like working groups with representative membership, white papers, and public consultations. Participation of marginalised groups and populations should be proactively ensured. Once collected, the data of individuals and communities is often reused and therefore health data governance must provide ongoing mechanisms for meaningful individual and community participation. This may include means for reaffirming consent when new data needs are defined, as well as ways to receive and address various inquiries and concerns from individuals and communities.

### **Connect to broader accountability mechanisms**

Health data governance should be integrated into formal public accountability mechanisms that may exist in a given context to ensure adherence to health-related policies, laws and rights. In addition, certain types of health data may be useful to, and made available for, monitoring and accountability efforts led by communities and civil society.



# ACKNOWLEDGEMENTS



Transform Health stewarded the development of the Health Data Governance Principles, under the leadership of its Policy Circle, whose members include: Marwa Azelmat (Young Experts: Tech 4 Health), Joseline Carias (Central American Health Informatics Network/RECAINSA), Marie Donaldson, Vikas Dwivedi and Vidya Mahadevan (Health Data Collaborative's Digital and Data Governance Working Group); Ulla Jasper (Fondation Botnar), Parminder Jeet Singh (IT for Change), Rigveda Kadam (FIND), Alice Liu (I-DAIR), Beatrice Murage (Philips/Digital Connected Care Coalition), Erica Troncoso (Jhpiego), and Jai Ganesh Udayasankaran (Asia eHealth Information Network/AeHIN).

This draft of the Health Data Governance Principles was prepared for Transform Health by Anna Volbrecht (PATH) and Akarsh Venkatasubramanian (Transform Health). Valuable inputs were provided by Transform Health colleagues, including Mathilde Forslund, Asmita Ghosh, Louise Holly, Kirsten Mathieson, and Frank Smith. PATH provided important contributions to this work, including Jacqueline Deelstra, Hallie Goertz, Kanishka Katara, Neema Ringo, Dykki Settle, and Anna Volbrecht. Other partners who provided inputs include: Ashley Bennett (Facebook, formerly PATH), Keertana Duppala (FIND), Mark Herringer (Healthsites), Riccardo Lampariello (Terre des Hommes),

Angélica Baptista Silva (Fiocruz), and Waruguru Wanjau (Kenya Medical Association).

The following partners were instrumental in supporting the global and regional consultations: PATH, AeHIN, the BID Learning Network, Mwan Events, RECAINSA, Wilton Park, the Lancet/FT Commission on Governing Health Futures 2030 and Young Experts: Tech 4 Health.

This work was funded by Fondation Botnar.



**healthdataprinciples.org**

Copyright © 2022, Transform Health. Some rights reserved. This work is licensed under the Creative Commons Attribution-Non-commercial-Share Alike 4.0 International License (CC BY-NC-SA 4.0). To view a copy of this licence, visit [creativecommons.org/licenses/by-nc-sa/4.0/legalcode](https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode) or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA. The content in this document may be freely used for non-commercial uses in accordance with this licence, provided the material is shared with a similar licence and accompanied by the following attribution: Transform Health. Health Data Governance Principles. Copyright © 2022, Transform Health.