Health Data Governance

Legislative and Regulatory Landscape Review

RWANDA

COUNTRY REPORT

Health Data Governance

Legislative and Regulatory Landscape Review

RWANDA

COUNTRY REPORT

This health data governance country landscape report was developed by Transform Health, with contributions from Vital Wave. 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.

Transform Health

Vital Wave℠

1. Introduction

This report analyses the legislative and regulatory landscape of Rwanda to understand how and to what extent the governance of health data is addressed. The Health Data Governance Principles (HDG Principles)[1] served as a framework for this analysis to explore and document how the principles manifest in the existing legal and regulatory environment. This review entailed a content analysis of relevant legal texts against the eight HDG Principles.

This review explores where Rwanda is in the process of developing legislative texts relevant to health data governance, including in domains such as digital health, primary health delivery, data privacy, cybersecurity, and emerging technologies.

In addition to the text review, the assessment draws from targeted interviews with in-country stakeholders working on digital health, data protection, legislation and regulation development, and data protection and cybersecurity oversight. These interviews provided additional context and insight into experience developing and operationalising laws and policies around health data governance.

Health Data Governance Principles

Protect People

- Protect individuals & communities
- Build trust in data systems
- Ensure data security

Promote health value

- Enhance health systems & services
- Promote data sharing & interoperability
- Enhance health systems & services

Prioritise equity

- Establish data rights & ownership
- Promote equitable benefit from health data

1 View the Health Data Governance Principles: https://healthdataprinciples.org

2. National legislative overview

This section provides a timeline and brief summary of legislation and regulation in Rwanda relevant to health data governance, which were identified and reviewed for this analysis.

Rwanda's Data Protection and Privacy Law (DPP)[2] is the primary legislation governing data privacy and protection. It aligns text and phrasing with the European Union's General Data Protection Regulation (GDPR), and other references.

There is no general health or primary healthcare law. Strategy documents and legally binding ministerial[3] instructions guide health system functioning, however, content on data governance is sparse. The Ministerial Instructions Governing Private Health Facilities is a Ministerial directive with content relevant to health data governance.

Rwanda's Cyber Crimes Law[4] creates a legal framework to prosecute cyber-related crimes. It focuses on fines and culpability rather than preventative security protocols more relevant to data governance. The National Cyber Security Authority (NCSA)'s legal standing granted through this law gives its "standards" and "directives" authority similar to regulations. The DPP's oversight body, the Data Protection Office, is also housed within the NCSA Rwanda has also ratified key regional and international conventions on human rights and cybersecurity.

While the Law governing the organisation of the Community-Based Health Insurance Scheme (CBHI) does not self-define as universal health coverage legislation, it serves a similar purpose. It articulates that those failing to enroll and not qualifying for assistance can be fined.

Rwanda is signatory to the African Union Convention on Cyber Security and Personal Data Protection (the "Malabo Convention")[5] and the African Charter on Human and Peoples' Rights.

2 https://dpo.gov.rw/dpp-law/

3 https://www.moh.gov.rw/index.php?eID=dumpFile&t=f&f=17768&token=4d040e80b0c19cfbb2b6e745efc-490b60128b40a

4 https://www.govca.rw/download/Law_on_prevention_and_punishment_of_cyber_crimes.pdf

5 https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

6 https://au.int/en/treaties/african-charter-human-and-peoples-rights

2021

Data Protection and Privacy Law (DPP)

2020

Ministerial Instructions Governing Private Health Facilities

2018

Cyber Crimes Law

2017

Law Establishing the Cyber Security Authority

2015

Law Governing the Organisation of the Community-Based Health Insurance Scheme

2008

Law Establishing the National Council of Nurses

Colour legend for legal texts

- General data protection
- Cybercrime
- Health
- Emerging Technology

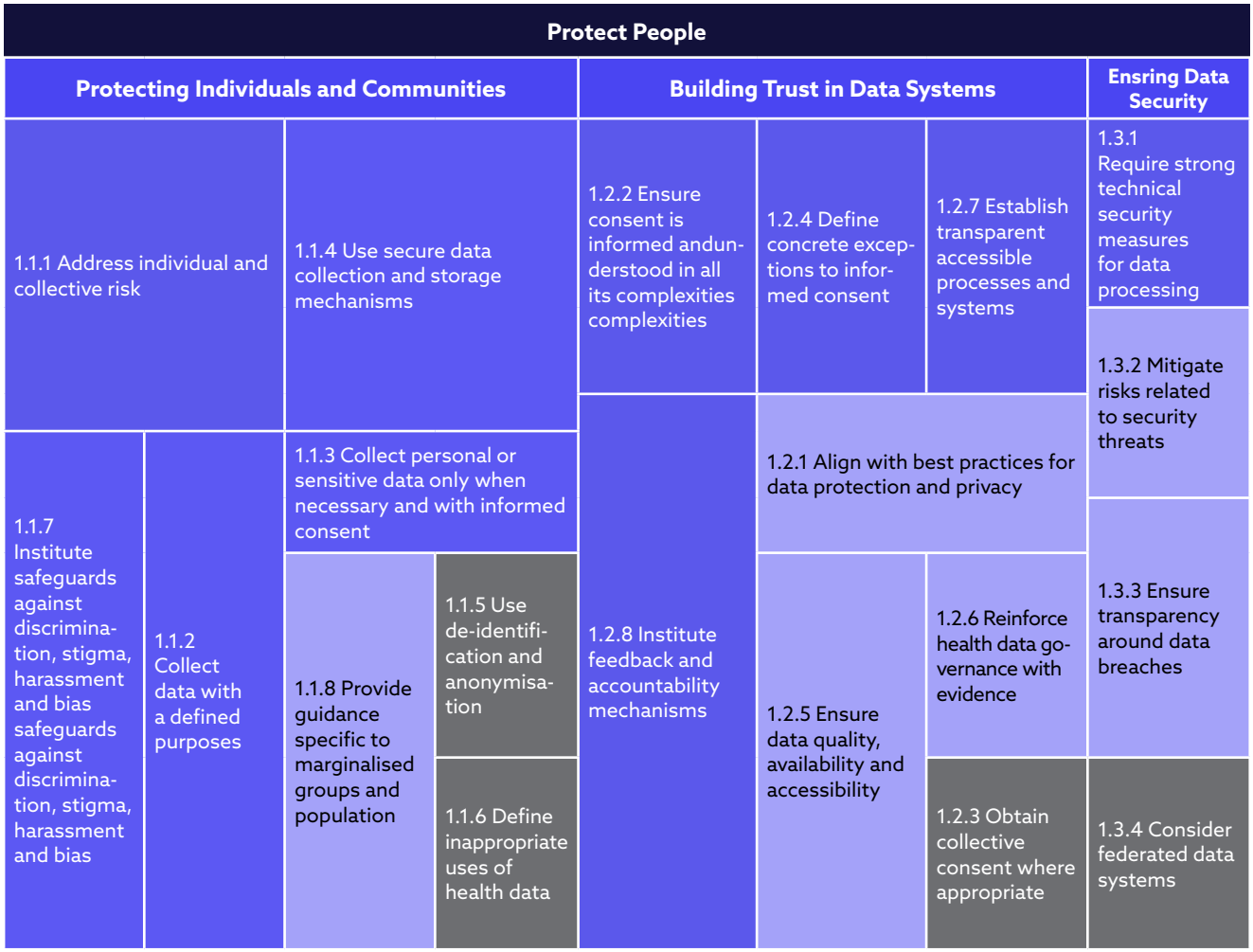
3. Analysis of the national legislative environment

This section highlights where the Health Data Governance Principles' core elements are reflected in the legal texts reviewed for the country. This is based on a content analysis of relevant legal texts.

3.1 Protect people

Rwanda's Data Protection and Privacy Law (DPP) includes significant language on data subject rights and informed consent, though collective consent and uses of health-specific data were absent from all reviewed text. The DPP includes definitions of key terms that ground the spirit of the law around individual risk mitigation. The DPP grounds itself in the understanding that the right to protection of personal information is a human right. It links the concept of data protection to the individual's right to information and freedom from discrimination. It is influenced by Kenya's and Mauritius' respective data privacy laws and the European Union's General Data Protection Regulation (GDPR).

The law establishing the National Cyber Security Authority (NCSA) and the Data Protection and Privacy and Cybercrimes law include common data protection requirements, though core elements regarding risk mitigation, transparency around data breaches, and reinforcing data with evidence are less frequent. The law establishing the NCSA grounds itself in a commitment to mitigate the collective risks of the nation (protecting national security and integrity). It is one of few references to collective risk, though not specific to health data and in reference to a national level "collective" rather than a community.



Key Findings Colour Code

Principle highlighted in **blue** were covered in the existing acts/regulation.
Principle highlighted in **light blue** were partially covered in the existing acts/regulation.
Principle highlighted in **gray** were not covered in the existing acts/regulation

3.2 Promote health value

Language on data sharing, particularly across borders, was the most common overlap with core elements in this category. Content on empowering frontline workers was absent. Rwanda's DPP overlaps with several core elements, including content regarding informed consent and applying data impact assessments to new technologies.

The 2020 ministerial instructions for private health facilities require hospitals to demonstrate compliance with requirements for ongoing data sharing, suggesting a reference to interoperability. It requires facilities to share data to support service delivery as a condition of licensure. It speaks to "using to enhance health services" by highlighting the center's need for facility-level data for decision-making.

The DPP establishes that sensitive personal data can be processed to improve health service delivery and longer-term statistical research for R&D. The DPP establishes that data subjects have the right not to be subject to a decision made only by automatic processing, including profiling. This provision does not apply if the controller establishes "suitable measures to safeguard" a subject's rights and interests, though 'suitable' is not defined.

The Anti-Cyber Crime Law's definitions of "electronic data" and "information technology" leave room for innovations and emerging technology. The former specifies "new technology" and the latter mentions actions associated with predictive algorithms and other AI.

<table>
<tr><th colspan="8">Promote Health Value</th></tr>
<tr><th colspan="4">Promote Data Sharing and Interoperability</th><th colspan="3">Enhance Health Systems and Services</th><th>Facilitate Innovation Using Health Data</th></tr>
<tr><td rowspan="3">2.2.1 Establish data sharing rules and guidelines</td><td colspan="3">2.2.7 Support multi-sector partnerships</td><td rowspan="2">2.1.1
Evaluate the benefits of health data</td><td rowspan="2">2.1.2 Use data to enhance health services for individuals and communities</td><td></td><td>2.3.1 Apply health data governance to emerging technologies</td></tr>
<tr><td rowspan="2">2.2.2 Validate informed consent before sharing data</td><td colspan="2">2.2.3 Promote interoperability of data systems</td><td colspan="2">2.3.3 Build public health data infrastructure</td></tr>
<tr><td rowspan="2">2.2.4 Define common data structures across health systems</td><td>2.2.5 Define multiple levels of data access</td><td rowspan="2">2.1.3 Encourage a culture of data-led insights and actions</td><td colspan="2">2.1.4 Address health system efficiency, effectiveness and resilience</td><td rowspan="2">2.3.4 Employ policy innovation</td><td rowspan="2">2.3.2 Address the use of non-health data in health contexts</td></tr>
<tr><td>2.2.6 Use common definitions and global standards</td><td>2.1.6 Enable and empower frontline health workers</td><td>2.1.5 Strengthen community ownership of health data</td></tr>
</table>

Key Findings Colour Code

Principle highlighted in **blue** were covered in the existing acts/regulation.
Principle highlighted in **light blue** were partially covered in the existing acts/regulation.
Principle highlighted in **gray** were not covered in the existing acts/regulation

3.3 Prioritise equity

Reviewed legislation and regulations included references to human rights, language accessibility, and identified governance roles and responsibilities. However, participatory governance and data bias mitigation were absent.

The DPP and the law establishing the NCSA outline responsibilities for Data Protection Officers and the NCSA, respectively, to establish and promote data privacy and cyber security education, awareness, and training programs. Both documents include language on ensuring accessibility and educating the population. Grounds for processing sensitive personal data in the DPP without consent extend to "ensuring high standards of quality and safety of medicinal products or medical devices." While governance roles are discussed, no reviewed texts specify connections to broader accountability mechanisms.

Gaps identified include language on health data trusts, participatory data governance, and inclusive feedback mechanisms.

<table>
<tr><th colspan="5">Prioritise Equity</th></tr>
<tr><th colspan="3">Establish Data Rights and Ownership</th><th colspan="2">Promote Equitable Benefits from Health Data</th></tr>
<tr><td rowspan="2">3.2.1 Apply a human rights lens to health data governance</td><td colspan="2">3.2.3 Codify data rights and ownership</td><td colspan="2">3.1.4 Use accessible language and plug knowledge gaps</td></tr>
<tr><td colspan="2">3.2.4 Extend data rights and ownership to products and services</td><td rowspan="3">3.1.6 Promote equitable impact and benefit</td><td>3.1.2 Consider the unique needs of marginalized groups and population</td></tr>
<tr><td rowspan="2">3.2.2 Define clear governance roles and responsibilities</td><td rowspan="2">3.2.7 Connect to broader accountability mechanism</td><td>3.2.5 Develop health data trusts and health data cooperatives</td><td rowspan="2">3.1.1 Represent all groups and populations equitably in data</td><td>3.1.3 Mitigate data bias</td></tr>
<tr><td>3.2.6 Employ participatory data governance mechanisms</td><td>3.1.5 implement inclusive data mechanisms</td></tr>
</table>

Key Findings Colour Code

Principle highlighted in **blue** were covered in the existing acts/regulation.
Principle highlighted in **light blue** were partially covered in the existing acts/regulation.
Principle highlighted in **gray** were not covered in the existing acts/regulation

Insights from Country Stakeholders

Open questions remain around ensuring c**ompliance from stewards of Rwandan data outside the country,** presenting challenges with respect to privacy, security, and ownership.

Low digital literacy is flagged as a primary obstacle to citizens being well-informed and confident about their data rights.

Interviews suggest a **balance** is needed between responsible national and cross-national data governance (adherence to data flow regulations and international frameworks) and ensuring laws **do not stifle innovation.**

Country leverages **multi-sector coordination** to design sector-specific data governance plans. Recently-introduced sandbox simulation then connects industry innovators and regulators to communicate risks on both sides.

Annex 1

Complete list of Health Data Governance Principles core elements

1. Protect People and Communities

1.1.1 Adress indivual and collective risk

1.1.2. Collect data with a defined purposes

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

1.1.4. Use secure data collection and storage mechanims

1.1.5 Use de-identification and anonymisation

1.1.6.Define inappropriate uses of health data

1.1.7. Institute safeguards against discrimination, stigma, harassment, and bias

1.1.8. Provide guidance specific to marginalised

groups and populations

1.2.1. Aling with best practices for data protection and privacy.

1.2.2. Ensure consent is informed and understood in all its complexities.

1.2.3. obtain collective consent where appropriate

1.2.4. Define concrete exceptions to informed consent

1.2.5. Ensure data quality, availability, and accessibility

1.2.6. Reinforce health data goverance with evidence

1.2.7. Establish transparent and accessible processes and systems

1.2.8. Institute feedback and accountability mechanisms

1.3.1. Require strong technical security measures for data processing

1.3.2. Mitigate risks related to security threals

1.3.3. Ensure transparency around data breaches

1.3.4. Consider federated data systems

2. Promote Health Value

2.1.1 Evaluate the benefits of health data

2.1.2. Use data to enhance health services for individuals and communietes

2.1.3. Encourage a culture af data -led insights and action

2.1.4 Adress health system efficiency, effectiveness, and resiliance

2.1.5. Strengthen community ownership of health data

2.1.6 Enable and empower frontifine health workers

2.2.1. Establish data sharing rules and guidelines

2.2.2. Validate informed consent before sharing data

2.2.3.Promote interoperability of data systems

2.2.4 Define common data structures across health systems

2.2.5 Define multiple levels of data access

2.2.7 Support multi-sector partneship

2.3.1. Apply health data goverance to emerging technologies

2.3.2. Adress the use of non- health data in health contexts

2.3.3. Build public health data infraestructure

2.3.4. Employ policy innovation

3. Prioritise Equity

3.1.1. Represent all groups and populations equitabably in data

3.1.2 Consider the unique needs of marginalised groups and populations.

3.1.3 Milgate date bias

3.1.4 Use accessible language and plug knowledge gaps.

3.1.5 Implement inclusive data feedback mechanisms

3.1.6 Promote equitable impact and benefit

3.2.1 Apply a human rigths lens to health data governance

3.2.2. Define clear goverance roles and responsabilities

3.2.3 Codify data rigths and ownership

3.2.4 Extend data rigths and ownership to products and services

3.2.5 Develop health data trust and health data cooperatives

3.2.6. Employ participatory data goverance mechanisms

3.2.7. Connect to broader accountability mechanisms