

Health Data Governance

Legislative and Regulatory
Landscape Review



SENEGAL
COUNTRY REPORT



Health Data Governance

Legislative and Regulatory
Landscape Review

SENEGAL
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.

Copyright © 2024, Transform Health. Some rights reserved. This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0). To view a copy of this license, visit 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 license provided the material is shared with a similar license and accompanied by the following attribution: "Transform Health. Health Data Governance Legislative and Regulatory Landscape Review: Senegal Country Summary Report. Basel: Transform Health, 2024."

1. Introduction

This report analyses the legislative and regulatory landscape of Senegal 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 Senegal 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 Senegal relevant to health data governance, which were identified and reviewed for this analysis.

Senegal's Data Protection Law (Law 2008/12 Concerning the Personal Data Protection)², was enacted in 2008. It lays out basic protections on personal data, including health.

Senegal's Cybercrime Law (Law 2008/11 on Cybercrime)³ is one of several sets of regulations governing implementation of the Data Protection Act and closely following the European Union's General Data Protection Regulation (GDPR). It focuses almost exclusively on penalties, with little content around security.

The draft Orientation Law on Digital Health⁴ has been drafted and includes significant detail on security and use of data in health. It has not yet been introduced as a bill.

Senegal 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' Rights⁶.



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.

2 https://www.dataguidance.com/sites/default/files/Senegal_data_protection_law_EN_1.pdf

3 <https://www.ictpolicyafrica.org/en/document/3zdepi6na5a?page=3>

4 <https://www.wearetech.africa/en/fils-uk/news/public-management/senegal-secures-nearly-50-mln-in-world-bank-funding-to-digitize-its-healthcare-system>

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>

Protect people

Senegal's 2008 Law on the Protection of Personal Data has been enacted for over a decade, with many of the same data subject rights seen in more recent data protection laws. It includes many concepts related to protecting individuals, which are also reinforced in the Malabo Convention. However, it has reportedly had little impact on practices in the health sector. It includes broad language about protecting the integrity of data, but is not technical or specific regarding security measures. The cybercrime law focuses on articulating crimes and penalties over security requirements.

Concepts relating to collective consent and specific data security measures are not present in current legislation. In contrast to several more recent data protection laws, specific approaches for data security, such as de-identification and anonymisation are not mentioned in any of the legal texts reviewed for Senegal.

Concepts not identified in the legal texts include consideration for collective consent; reinforcing health data governance with evidence; specific consideration of federated data systems; and specific requirements to report data breaches and mitigate security risks.

Protect People							
Protecting Individuals and Communities			Building Trust in Data Systems		Ensuring Data Security		
1.1.1 Address individual and collective risk		1.1.7 Institute safeguards against discrimination, stigma, harassment and bias safeguards against discrimination, stigma, harassment and bias		1.2.8 Institute feedback and accountability mechanisms	1.2.4 Define concrete exceptions to informed consent	1.3.1 Require strong technical security measures for data processing	
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 mechanisms		1.2.5 Ensure data quality, availability and accessibility	1.2.2 Ensure consent is informed and understood in all its complexities complexities		
		1.1.6 Define inappropriate uses of health data	1.1.5 Use de-identification and anonymisation		1.2.1 Align with best practices for data protection and privacy	1.2.7 Establish transparent accessible processes and systems	1.2.3 Obtain collective consent where appropriate
			1.1.8 Provide guidance specific to marginalised groups and population				1.2.6 Reinforce health data governance with evidence
						1.3.2 Mitigate risks related to security threats	
						1.3.3 Ensure transparency around data breaches	
						1.3.4 Consider federated data systems	

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



Promote health value

Given the absence of a robust health law in Senegal, there is little in the legal landscape that corresponds to “promoting health value”. One exception is considerations for protecting data to be shared across borders, which is contained in articles of the law concerning Personal Data Protection containing. Similar to other general data protection laws, Senegal’s personal data protection law requires data controllers to only transfer data if

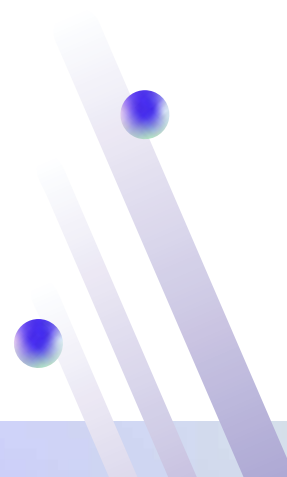
the receiving entity can sufficiently protect rights and freedoms of the persons whose data will be transferred.

The draft orientation law on digital health is expected to include more specificity than the data protection law in the context of using health-specific data.

Promote Health Value					
Promote Data Sharing and Interoperability		Enhance Health Systems and Services		Facilitate Innovation Using Health Data	
2.2.1 Establish data sharing rules and guidelines	2.2.3 Promote interoperability of data systems	2.2.4 Define common data structures across health systems	2.1.1 Evaluate the benefits of health data	2.1.2 Use data to enhance health services for individuals and communities	2.3.1 Apply health data governance to emerging technologies
	2.2.2 Validate informed consent before sharing data	2.2.5 Define multiple levels of data access	2.2.6 Use common definitions and global standards	2.1.3 Encourage a culture of data-led insights and actions	2.1.4 Address health system efficiency, effectiveness and resilience
2.2.7 Support multi-sector partnerships			2.1.5 Strengthen community ownership of health data		2.1.6 Enable and empower frontline health workers
					2.3.4 Employ policy innovation

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



Prioritise equity

Senegal's data protection and cyber crime laws reference the human right to access to care and broadly promote equitable benefit of health outcomes. The Personal Data Protection law requires one member of the Data Protection Commission to be from an organisation that has a human rights position.

None of the reviewed texts discussed considerations for data ownership and equity in data use. Both the 2008 law on protection of data and the AU Malabo Convention codify data subject rights but include little specific text around ownership. There were no specific references to participatory processes for health data governance, consideration of data trusts and cooperatives, and many specifics around promoting equitable benefit from health data.

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

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



Partners are working to **build technical and infrastructure capacity** to support data governance over the next decade.



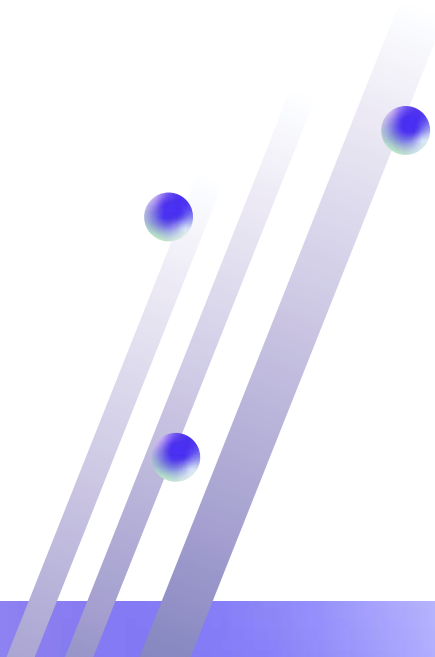
Draft data protection law is seen as a **necessary framework** to curb a highly fragmented landscape of information systems and redundant applications currently in use.



Infrastructure constraints limit the country's ability to host data locally, despite intent. Slight **adjustment to current phrasing** in data protection law, such as "data can be hosted on local servers and on the cloud," can support a development pathway.



Developing region-specific guidance may **unnecessarily fragment** approaches to health data governance. Health data governance is affecting everyone, and geography and language shouldn't be the main drivers of how discussions about health data governance occur.



Annex 1

Complete list of Health Data Governance Principles core elements

1. Protect People and Communities

- 1.1.1 Address individual 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 mechanisms
- 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. Align 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 governance 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 threats
- 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 communities
- 2.1.3. Encourage a culture of data-led insights and action
- 2.1.4 Address health system efficiency, effectiveness, and resilience
- 2.1.5. Strengthen community ownership of health data
- 2.1.6 Enable and empower frontline 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 partnership
- 2.3.1. Apply health data governance to emerging technologies
- 2.3.2. Address the use of non-health data in health contexts
- 2.3.3. Build public health data infrastructure
- 2.3.4. Employ policy innovation

3. Prioritise Equity

- 3.1.1. Represent all groups and populations equitably in data
- 3.1.2 Consider the unique needs of marginalised groups and populations.
- 3.1.3 Mitigate data 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 rights lens to health data governance
- 3.2.2. Define clear governance roles and responsibilities
- 3.2.3 Codify data rights and ownership
- 3.2.4 Extend data rights and ownership to products and services
- 3.2.5 Develop health data trust and health data cooperatives
- 3.2.6. Employ participatory data governance mechanisms
- 3.2.7. Connect to broader accountability mechanisms