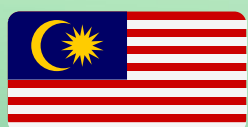


Health Data Governance

Legislative and Regulatory
Landscape Review



MALAYSIA
COUNTRY REPORT

Health Data Governance

Legislative and Regulatory
Landscape Review

MALAYSIA
COUNTRY REPORT

This health data governance country landscape report was developed by Transform Health, with contributions from the Asia eHealth Information Network (AeHIN). 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: Malaysia Country Summary Report. Basel: Transform Health, 2024."

1. Introduction

This report analyses the legislative and regulatory landscape of Malaysia to understand how and to what extent the governance of health data is addressed. The Health Data Governance Principles¹ were used as a framework for this analysis, to explore and document how the principles manifest in the existing legal and regulatory environment. This entailed a content analysis of relevant legal texts against the eight principles, the most specific sub-level under the HDG Principles' three broad objectives to Protect People, Promote Health Value, and Prioritise Equity.

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



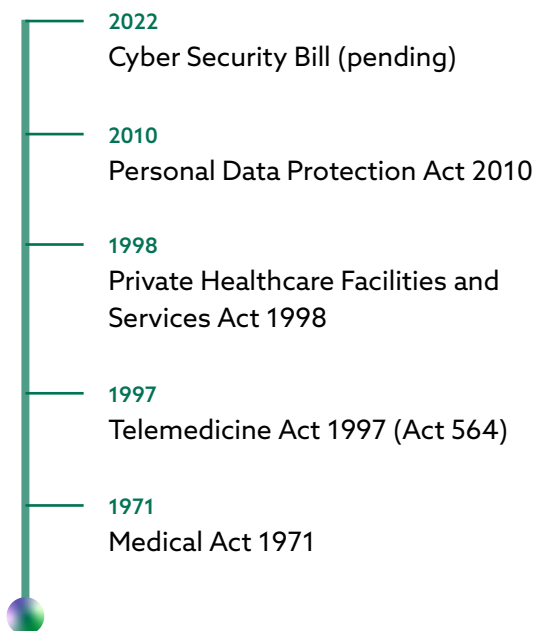
Promote equitable benefit from health data

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 Malaysia relevant to health data governance, which were identified and reviewed for this landscape. This provides the basis for the content analysis that follows.

In Malaysia, the Acts and regulations with a focus on health date back in 1971, with the Medical Act². This subsequently proceeded to Acts and regulations focusing on telemedicine (1997)³, and on healthcare facilities and services (1998)⁴. The Telemedicine Act 1997⁵ covers the practice of medicine using audio, visual and data communications. The Personal Data Protection Act⁶, which was released in 2010, includes health data as “sensitive data” in its definitions. There are no current Acts specific to digital health or artificial intelligence domains.



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.

The Malaysia Personal Data Protection Act 2010 defines health data as “sensitive personal data” and the governance of it has been included. It also includes explicit definitions on “healthcare services” and “healthcare professionals”. Telemedicine Act 1997 aims to regulate and control the practice of telemedicine.

2 <https://mmc.gov.my/wp-content/uploads/2022/06/Medical-Act-1971.pdf>

3 <https://www.moh.gov.my/moh/attachments/1205.pdf>

4 https://www.moh.gov.my/index.php/database_stores/attach_download/317/27

5 <https://www.moh.gov.my/moh/attachments/1205.pdf>

6 <https://www.malaysia.gov.my/portal/content/654>

Protect people

In terms of protecting individuals and communities, the Personal Data Protection Act 2010 defines health data as “sensitive personal data” and contains statements on how it should be processed, which includes consent, storage, and how data can be shared.

With regard to building trust in data systems, the Telemedicine Act 1997 highlights the need for consent from patients before sharing any information or image via telemedicine interaction to any research or any other person. This will help to build trust for practicing telemedicine.

To help ensure data security, the Personal Data Protection Act 2010 lists security principles for data users in section nine. It also contains provisions to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

Protect People						
Protecting Individuals and Communities			Building Trust in Data Systems			
1.1.1 Address individual and collective risk		1.1.4 Use secure data collection and storage mechanisms		1.2.5 Ensure data quality, availability and accessibility	1.2.1 Align with best practices for data protection and privacy	
1.1.7 Institute safeguards against discrimination, stigma, harassment and bias	1.1.2 Collect data with a defined purposes	1.1.3 Collect personal or sensitive data only when necessary and with informed consent	1.2.8 Institute feedback and accountability mechanisms	1.2.4 Define concrete exceptions to informed consent	1.2.7 Establish transparent accessible processes and systems	
		1.1.6 Define inappropriate uses of health data	1.2.2 Ensure consent is informed and understood in all its complexities		1.2.3 Obtain collective consent where appropriate	
		1.1.5 Use de-identification and anonymisation	1.1.8 Provide guidance specific to marginalised groups and population	Ensuring Data Security		
				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
					1.2.6 Reinforce health data governance with evidence	
					1.3.4 Consider federated data systems	

Key Findings Colour Code

Principle highlighted in **green** were covered in the existing acts/regulation.
 Principle highlighted in **gray** were not covered in the existing acts/regulation



Promote health value

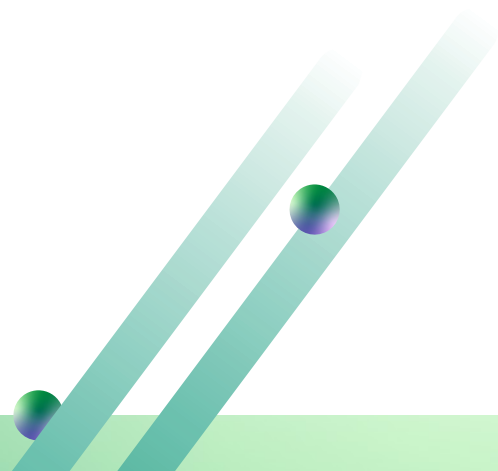
Towards enhancing health systems and services, the Private Healthcare Facilities and Services Act 1998 promotes the quality of health services by stating in Section 74 that “every private healthcare facility or service shall have programmes and activities to ensure the quality and appropriateness of healthcare facilities and services provided.”

In relation to promoting data sharing and interoperability, the Personal Data Protection Act 2010 includes the need for data requests in order to obtain the data. There was no mention about interoperability or standards.

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

Key Findings Colour Code

Principle highlighted in **green** were covered in the existing acts/regulation.
 Principle highlighted in **gray** were not covered in the existing acts/regulation



Prioritise equity

When it comes to establishing data rights and ownership, the Private Healthcare Facilities and Services Act 1998 includes provisions regarding a patient’s right to their records and in relation to healthcare services provided by any healthcare facility or service, including privacy, confidentiality of information and access to patients’ medical reports and records. The Personal Data Protection Act 2010 included a section on “right of access

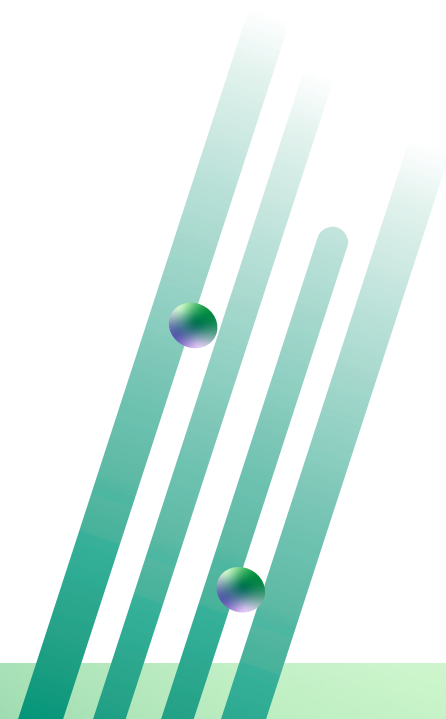
to personal data” where a data access request is needed with certain requirements to access the data from the data users. However, data users do not hold the personal data but rather control the process.

The current legislative landscape does not facilitate the promotion of equitable benefits from health data.

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

Key Findings Colour Code

Principle highlighted in **green** were covered in the existing acts/regulation.
 Principle highlighted in **gray** were not covered in the existing acts/regulation



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

