Health Data Governance

Legislative and Regulatory Landscape Review

SINGAPORE

COUNTRY REPORT

Health Data Governance

Legislative and Regulatory Landscape Review

SINGAPORE

COUNTRY REPORT

This health data governance country landscape report was developed by Transform Health, with contributions from Research ICT Solutions and Baker Botts. 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

1. Introduction

This report analyses the legislative and regulatory landscape of Singapore 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 report identifies best practices for Singapore's health data governance, including recommendations on how to strengthen its existing health data governance legislative and regulatory landscape. It highlights the multifaceted approach Singapore takes in safeguarding personal and health data through constitutional provisions, specific legislation, cybersecurity measures, and governmental guidelines. It underscores the establishment of trust in data systems via legislative acts, regulations, and guidelines that foster transparency, accountability, and security across various sectors. Additionally, the report points out the comprehensive measures in place for data security, emphasising obligations for organisations and government agencies to protect data against unauthorised access and breaches.

This report lays the foundation for an in-depth analysis of Singapore's health data governance legislation and regulations. Drawing from a diverse range of sources, including the Constitution of the Republic of Singapore, the Personal Data Protection Act, the Healthcare Services Act, and the Cybersecurity Act, among others, the report aims to dissect and evaluate the existing regulatory frameworks. These sources provide a comprehensive backdrop for understanding the intricacies of Singapore's approach to health data governance.

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

2. National Legislative and Regulatory Overview

The following sources were used for purposes of analysing the legislative and regulatory system of Singapore:

- Constitution of the Republic of Singapore, 1965 (2020 rev. ed.)
- Personal Data Protection Act 2012, Act 26 of 2012 (Sing.)
- Personal Data Protection (Notification of Data Breaches) Regulations 2021, S 48/2021 (Sing.)
- Healthcare Services Act 2020, Act 3 of 2020 (Sing.)
- Cybersecurity Act 2018, Act 9 of 2018 (Sing.)
- Intellectual Property Office of Singapore Act 2001, Act 3 of 2001 (Sing.)
- Telecommunications Act 1999, Act 43 of 1999 (Sing.)
- Personal Data Protection (Amendment) Act 2020 (Act 40 of 2020) (Sing.)
- Gov't of Sing., Personal Data Protection Policies (July 2021)
- Ministry of Health (Sing.), Guidelines on Appropriate Use and Access to National Electronic Health Records (NEHR) (2019)
- Woo Jun Jie, *Singapore's Smart Nation Initiative – A Policy and Organisational Perspective*, NUS Libraries (2017)
- Personal Data Protection Comm'n (Sing.), Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Sept. 23, 2013, rev'd May 16, 2022)
- Singapore Medical Council, Ethical Code and Ethical Guidelines (2016 ed.)
- Singapore Medical Council, Handbook on Medical Ethics (2016 ed.)
- M. Ramesh & Azad Singh Bali, The Healthcare System in Singapore, in Great Policy Successes 42 (2019)
- Comparing Privacy Laws: GDPR v. Singapore's PDPA, OneTrust DataGuidance (2022)
- Data Protection Laws of the World: Singapore, DLA Piper (Dec. 20, 2023)

3. Analysis of the National Legislative and Regulatory Environment

The currently enacted or most recently published legislative and regulatory instruments in Singapore relating to the eight HDG Principles are discussed under the sub-heading of each respective principle below.

3.1. Protect individuals and communities

Singapore's regulatory framework for protecting individuals and communities revolves around various laws and regulations addressing health and personal data protection. While the Constitution doesn't explicitly mention health or personal data, articles such as Liberty of the Person (Article 9) and Equal Protection (Article 12) indirectly contribute to personal liberty and privacy. The Personal Data Protection Act 2012 (PDPA) outlines obligations for organisations regarding the handling of personal data, including general rules, collection, use, disclosure, access, correction, care of personal data, and notification of data breaches. The Healthcare Services Act 2020 emphasises the confidentiality of medical information and outlines circumstances for disclosure, while the Cybersecurity Act 2018 protects critical systems and data, including health and personal information.

Additionally, the Intellectual Property Office of Singapore Act 2001 mandates secrecy regarding information obtained in the performance of duties, and the Telecommunications Act regulates the protection of personal data by telecommunication licensees. Various amendments and guidelines to the PDPA enhance personal data protection and accountability, including provisions for data breaches, data portability, and offences affecting personal data. Government guidelines and policies emphasise principles such as consent obligation, purpose limitation, protection obligation, and data breach notification obligation. Ethical guidelines for medical practitioners ensure responsible handling of patient information, including maintaining clear medical records and medical confidentiality.

The Smart Nation Initiative focuses on digitisation with an emphasis on cybersecurity and data privacy, ensuring a safe digital transformation. In summary, Singapore's regulatory framework employs a multi-faceted approach, encompassing constitutional provisions, specific legislation like the PDPA and Healthcare Services Act, cybersecurity measures, intellectual property regulations, telecommunications laws, and government guidelines, all aimed at safeguarding the privacy and security of individuals' health and personal data.

3.2. Building Trust in Data Systems

Additionally, certain laws and regulations seek to foster the public's trust in data systems generally. Foundational principles such as the rule of law, transparency, and accountability, as outlined in the Constitution of the Republic of Singapore, indirectly contribute to this trust. The Personal Data Protection Act 2012 (PDPA) plays a crucial role, with sections establishing the functions of the Personal Data Protection Commission, responsibilities of organisations, and requirements for policies and practices to ensure compliance. Similarly, the Healthcare Services Act 2020, though not specifying exact sections, includes provisions related to data privacy and security measures, contributing to trust in healthcare data systems.

The Cybersecurity Act 2018, particularly Section 11, establishes codes of practice and standards for critical information infrastructure owners, directly enhancing cybersecurity and trust in data systems. The Intellectual Property Office of Singapore Act 2001 and the Telecommunications Act of 1999 also contribute by setting standards for the responsible handling and dissemination of information and operational integrity, respectively. The Personal Data Protection (Amendment) Act 2020 introduces obligations for data breaches and data portability, reinforcing trust through enhanced accountability and protection measures. Government directives and guidelines, such as the IM on ICT&SS Management and PSGA, outline policies for managing and protecting data, ensuring transparency and legal compliance.

Additionally, initiatives like the Smart Nation Initiative emphasise cybersecurity and data privacy measures, essential for fostering trust in digital services and systems. The guiding principles on accessing medical records on the NEHR ensure responsible access to healthcare data, while the Ethical Code and Ethical Guidelines of the Singapore Medical Council emphasise secure medical records, vital for patient trust. Guidelines related to the GDPR and PDPA establish standards for trustworthy data handling practices, and tools like the Data Protection Management Program and Data Protection Impact Assessment Guides aid organisations in managing and protecting personal data effectively, thereby enhancing trust in data handling practices across various sectors.

3.3. Ensuring Data Security

Data protection and general cybersecurity are both touched upon by some Singapore laws, though there is limited regulation specifically directed to the use of health data. The PDPA is central to this framework, outlining obligations for organisations regarding the security and protection of personal data, including requirements for notifying data breaches. The Healthcare Services Act 2020 mandates licensees to implement safeguards for protecting healthcare records and computer systems, while the Personal Data Protection (Amendment) Act 2020 requires organisations to implement reasonable security arrangements for personal data protection. Additionally, the guidelines on the appropriate use and access to NEHR emphasise security principles for healthcare systems and data, and the Singapore Smart Nation Initiative recognises cybersecurity and data privacy as key components for sustaining innovation.

Other elements of the framework include the responsibilities of public officers in handling personal data, technical and process measures for data protection, and specific sections regarding medical confidentiality, which emphasise the secure storage and transmission of medical information. Although the Constitution of the Republic of Singapore and the Telecommunications Act 1999 do not explicitly address data security, the overall regulatory environment ensures that organisations, government agencies, and individuals are obligated to implement measures to safeguard data against unauthorised access, breaches, and misuse. The Advisory Guidelines on Key Concepts in the PDPA further reinforce the requirement for organisations to adopt reasonable security arrangements, ensuring a robust approach to data protection across various sectors.

3.4. Enhancing Health Services and Systems

The regulatory framework addressing the enhancement of health services and systems in Singapore involves several legislative acts, regulations, and guidelines. The Constitution of the Republic of Singapore provides the governance framework but lacks specific provisions for health services enhancement. The PDPA and its amendments, along with the Personal Data Protection (Notification of Data Breaches) Regulations 2021, focus on data protection, indirectly impacting healthcare through personal data handling. The Healthcare Services Act 2020 directly addresses healthcare service quality through licensing, duties of licensees, and compliance monitoring. The Cybersecurity Act 2018 ensures the cybersecurity of essential services, including public health services, while the Telecommunications Act supports health services through improved communication infrastructures.

Guidelines and initiatives also play a crucial role in enhancing health services. The NEHR Guidelines ensure ethical and effective use of patient data, while the Smart Nation Initiative aims to digitise and improve public services, including healthcare. Professional Conduct Guidelines emphasise health professionals' obligation to maintain fitness to practice, benefiting patient welfare. Clinical Care Guidelines outline principles for good clinical care, fundamental to enhancing health services. Healthcare reform measures include hospital restructuring, fiscal tools for affordability, regulatory measures, and information tools to improve healthcare efficiency, affordability, and quality. The glossary of terms, particularly the definition of "Evaluative Purpose," supports the use of personal data to improve health services and systems.

3.5. Promoting Data Sharing and Interoperability

Interoperability underpins several aspects of Singapore's regulatory framework. The PDPA, particularly Section 10, facilitates cooperation agreements between the Personal Data Protection Commission (PDPC) and other regulatory authorities to enhance data sharing practices. The Healthcare Services Act 2020, especially Sections 36 and 37, establishes a framework for gathering and disseminating health-related data, promoting interoperability among healthcare providers. The Cybersecurity Act 2018, through sections such as 11 and 14-16, regulates owners of Critical Information Infrastructure (CII) to ensure cybersecurity standards and incident reporting, fostering data sharing. The Telecommunications Act 1999, in Sections 5 and 6, addresses licensing and spectrum rights, setting conditions for interconnection and sharing of telecommunication systems and radio frequency spectrum. Additionally, the Intellectual Property Office of Singapore (IPOS) plays a role in managing and disseminating intellectual property information, indirectly contributing to data sharing and interoperability.

Further, the NEHR Guidelines, through Sections 3, 4, and 5, establish principles for contributing to, accessing, and using NEHR data, promoting secure and responsible data sharing among healthcare professionals. The Smart Nation Initiative emphasises data sharing through open data portals and platforms, supporting interoperability to drive innovation and development. Collectively, these legislative acts, regulations, and guidelines form a comprehensive regulatory framework that promotes data sharing and interoperability across various sectors in Singapore.

3.6. Facilitating Innovation using Health Data

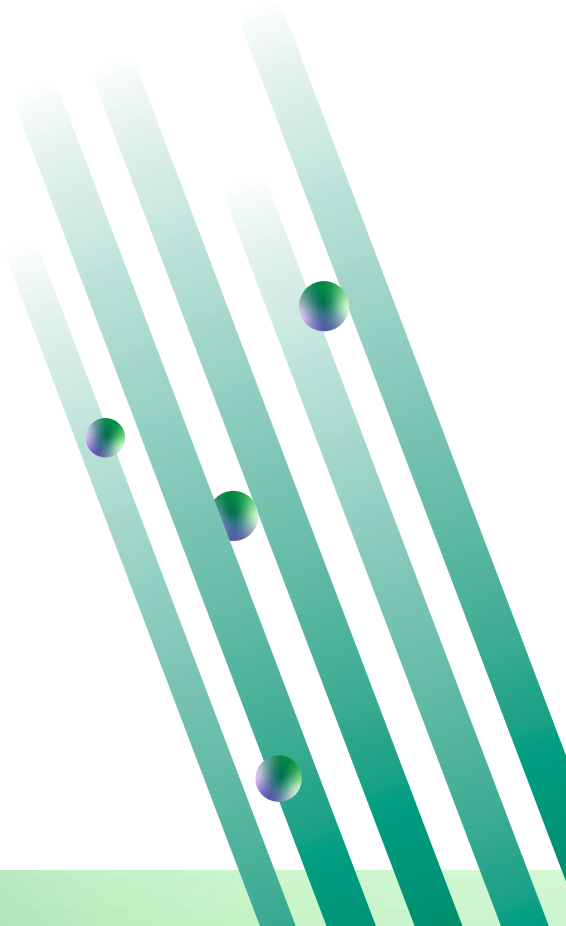
Singapore has few regulations directly addressing the facilitation of innovation using health data, but several elements indirectly influence this goal. The PDPA governs the collection, use, and disclosure of personal data, with provisions related to consent, anonymisation, and exceptions that could indirectly support innovative uses of health data. The Healthcare Services Act 2020, while not directly addressing innovation, includes regulations concerning the governance of healthcare services, data privacy, and technology use in healthcare provision, which indirectly impact innovation using health data. The Intellectual Property Office of Singapore Act 2001, particularly sections 6 and 7, supports innovation by promoting public awareness, advising the government on intellectual property matters, and engaging in technical cooperation in the area of intellectual property. Additionally, the Smart Nation Initiative fosters a culture of experimentation and innovation, including in health, by enabling data sharing, investing in R&D, and creating 'living laboratories' for piloting technological solutions.

3.7. Promoting Equitable Benefits from Health Data

The regulatory framework concerning the promotion of equitable benefits from health data in Singapore is governed by various acts and regulations. The Constitution outlines the fundamental structure of governance and individual rights but does not specifically address health data. The Healthcare Services Act 2020 indirectly contributes to equitable health data use through provisions related to licensing, duties of licensees, and compliance monitoring, ensuring regulated and ethical healthcare service delivery. The PDPA establishes guidelines for the collection, use, and disclosure of personal data, emphasising consent, data portability, and data breach notification requirements, thereby indirectly promoting equitable benefits from health data.

The NEHR Guidelines ensure high-quality patient care, confidentiality, and privacy while facilitating appropriate use and access to electronic health records. The Smart Nation Initiative aims to digitise urban life, including healthcare, through collaborations and experimentation to enhance living standards and economic productivity, thereby promoting equitable benefits from health data.

Additionally, Ethical Guidelines for Medical Practice emphasise fair and equitable treatment of patients, indirectly supporting equitable benefits from health data by ensuring ethical standards in patient care and medical research. The integration of information tools in healthcare aims to harmonise healthcare processes and provide information on costs and outcomes, enabling patients to make informed choices. While there may not be explicit sections solely dedicated to promoting equitable benefits from health data in each document, the combination of these regulatory frameworks establishes a comprehensive approach to ensure the fair and ethical use of health data for the benefit of all stakeholders in Singapore's healthcare system.



3.8. Establishing Data Rights and Ownership

The regulatory framework in Singapore addressing data rights and ownership is primarily established through specialised legislation and policy documents rather than the Constitution. Key acts include the PDPA, which focuses on the collection, use, and disclosure of personal data, particularly in Part 4, covering consent and purpose. The PDPA also grants individuals rights to erasure, access, and personal data portability. The Healthcare Services Act 2020, in Part 7, Section 51, pertains to the confidentiality of medical information, indirectly implying data ownership. The Cybersecurity Act 2018 ensures cybersecurity standards and resilience of critical information infrastructure, while the Intellectual Property Office of Singapore Act 2001 relates to data rights through intellectual property systems and regulations. The Telecommunications Act 1999 regulates telecommunications systems and services, with data protection aspects potentially covered under separate legislation.

Government policies also play a significant role in data rights and ownership. The Government Personal Data Protection Policies of July 2021 establish guidelines for government agencies on the collection, use, and disclosure of personal data. The NEHR guidelines outline principles for the contribution, access, and use of health information, establishing ownership and management frameworks within the healthcare sector. Singapore's Smart Nation Initiative emphasises digital governance and policies for the country's digital transformation, although it does not isolate data rights and ownership.

4. Best practices

Singapore's regulatory framework for health data governance incorporates several best practices that ensure data security, privacy, and efficiency in healthcare delivery:

- **Robust Data Protection Legislation:** The Personal Data Protection Act 2012 (PDPA), together with its subsequent amendments, provides a comprehensive foundation for safeguarding personal health data. The PDPA mandates clear obligations for organisations on the collection, use, and disclosure of personal data, prioritising individual privacy while enabling the responsible use of data for healthcare delivery.
- **Mandatory Breach Notifications:** Under the Personal Data Protection (Notification of Data Breaches) Regulations 2021, organisations must report data breaches to the Personal Data Protection Commission (PDPC) and affected individuals when harm is likely, ensuring transparency and accountability.
- **Integration of Ethical Standards in Healthcare:** The Singapore Medical Council Ethical Code and Ethical Guidelines (2016) underscores the importance of patient confidentiality, informed consent, and professional accountability, ensuring that health data use aligns with medical ethics.
- **Promotion of Interoperability and Efficiency:** Singapore's Healthcare Services Act 2020 and the Guidelines on Appropriate Use and Access to National Electronic Health Records (NEHR) encourage the use of integrated systems for efficient healthcare delivery, reducing redundancies and improving outcomes.
- **Risk-Based Governance:** The framework promotes risk-based approaches, requiring organisations to conduct regular risk assessments and implement technical safeguards such as encryption, secure storage, and access controls.
- **Emphasis on Continuous Improvement:** Singapore's Smart Nation Initiative promotes innovation in health informatics through the adoption of digital health tools and electronic records, ensuring a forward-looking regulatory framework that adapts to evolving technological landscapes.

5. Gaps

Even in light of the above analysis and best practices, there still remain a number of gaps in Singapore's regulatory landscape with respect to health data.

- **Limited Proactive Security Standards:** The current regulations, while strong on breach notifications, lack explicit, prescriptive measures for preventing data breaches, leaving organisations to interpret general obligations.
- **Insufficient Guidance on Consent Mechanisms:** The PDPA requires consent but provides limited granularity on obtaining explicit, informed, or dynamic consent specific to health data, which could lead to inconsistent practices in sensitive areas like research or secondary data use.
- **Ambiguities in Cross-Border Data Transfers:** Although the PDPA includes requirements for overseas transfers, there is insufficient guidance on the adequacy of safeguards for cross-border health data sharing, creating compliance challenges for global healthcare collaborations.
- **Lack of Health-Specific Data Safeguards:** Existing regulations treat health data under the broader personal data category, without tailored protections for uniquely sensitive categories such as genetic or biometric data.
- **Insufficient Transparency in Data Use for Research:** Guidelines for using health data in medical research lack clarity, which could hinder research initiatives while maintaining compliance with ethical standards.
- **Limited Private Sector Integration:** Private healthcare providers often operate under fragmented systems, leading to inefficiencies and reduced interoperability with public systems such as NEHR.

6. Recommendations

To enhance the framework and address identified gaps, the following recommendations are proposed:

- **Introduce Prescriptive Data Security Standards:** Establish detailed technical and organisational measures for health data security, including minimum standards for encryption, anonymisation, and secure access.
- **Strengthen Consent Mechanisms:** Require explicit and dynamic consent for health data collection, with detailed guidelines tailored to healthcare contexts, including consent for research and secondary uses.
- **Expand Cross-Border Data Transfer Guidelines:** Provide clear criteria for assessing the adequacy of protections in destination jurisdictions for cross-border health data sharing, aligning with global best practices.
- **Create Health-Specific Data Protections:** Implement additional safeguards for sensitive categories like genetic and biometric data, recognising their unique risks and implications for individual privacy.
- **Clarify Research Data Use Standards:** Develop comprehensive guidelines for ethical and compliant use of health data in research, ensuring transparency and individual rights.
- **Enhance Private Sector Integration:** Mandate interoperability standards for private healthcare providers to ensure seamless integration with national systems like NEHR.
- **Strengthen Monitoring and Enforcement:** Allocate additional resources to the PDPC for proactive monitoring and establish stricter penalties for non-compliance with health data regulations.
- **Promote Health Data Literacy:** Introduce initiatives to educate the public on their data rights and responsibilities under the PDPA, fostering informed engagement in healthcare systems.

7. Discussion of Research Results

Singapore's health data governance reflects a commitment to balancing individual privacy rights with the benefits of data-driven healthcare innovation. The current regulatory framework incorporates foundational protections, ethical guidelines, and interoperability goals but reveals gaps in proactive security measures, consent mechanisms, and health-specific data protections. Addressing these gaps through targeted reforms can further enhance public trust, regulatory compliance, and the efficiency of Singapore's healthcare system.

8. Conclusion

Singapore's health data regulatory framework exemplifies a progressive approach to data governance, blending strong privacy safeguards with support for technological innovation. However, to maintain its leadership in health informatics and adapt to emerging challenges, the framework must evolve to include more detailed security standards, dynamic consent mechanisms, and health-specific protections. With these enhancements, Singapore can strengthen its healthcare ecosystem while safeguarding individual rights, ensuring that its policies align with both global standards and local needs.