MINISTRY OF HEALTH
SINGAPORE

Singapore's Perspective in Digital Health Regulations

EPSO Conference

31 May 2024

Healthier SG

An initiative of

FORWARD SG

Agenda

A. Singapore's Proposed Health Information Bill
B. Cybersecurity Labelling Scheme (Medical Devices)
C. Singapore's Approach towards Regulating AI

Singapore's healthcare operating context is changing

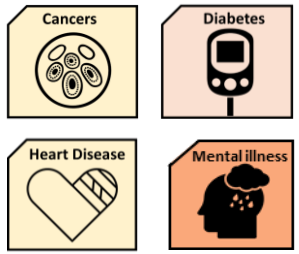
AGING POPULATION

By 2030,

- **1 in 4 Singaporeans aged ≥65**
- **OASR drop from 10.5 (in 1990) to 2.7**

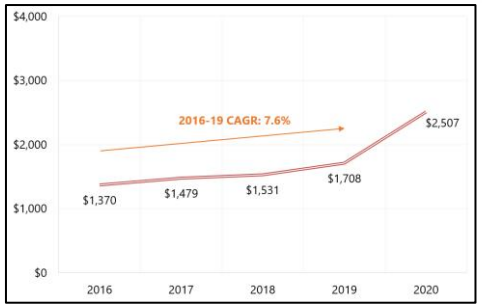
- Long lifespan and low birth rates of Singaporeans have led to **declining** old-age support ratio (OASR).

RISING INCIDENCE OF CHRONIC DISEASES



- Rising rates of chronic disease and age-related conditions such as neurological conditions and mental illness

INCREASING HEALTHCARE COSTS



- Driven by the ageing population and Government's shift to bear a greater proportion of healthcare costs

ADVANCING MEDICAL TECHNOLOGIES

- Personalised medicine via genetics and Precision Medicine
- Integration of AI technologies for clinical decision making

CONTINUED RISE OF HEALTHCARE CONSUMERISM

- With high mobile penetration rates, Singaporeans are increasingly becoming more digitalized
- Consumers getting more involved in their healthcare

CHANGING CARE MODELS

- New care models and services for patients (e.g., telemedicine)
- Need to regulate healthcare services beyond premises

Healthcare in Singapore is becoming more complex with care being provided in multiple settings

Shifting healthcare focus to preventive care is difficult but right thing to do, says PM Lee

The Straits Times

24 Apr 2022

Sep 2022

Age Well SG

Aug 2023

THE STRAITS TIMES

Subsidised hospital care in the comfort of home from April 1; new hospital in Tengah by early 2030s

Apr 2024

Regardless of where residents receive care, their healthcare providers should be able to retrieve accurate, up-to-date information for better care delivery

NEHR
National Electronic Health Record Singapore

The NEHR system captures selected key health information in a central platform, for easy access by licensed healthcare providers and healthcare professionals.

Health Information Bill

This Bill will mandate licensed healthcare providers contribute a copy of selected key health information (as determined by MOH) to the NEHR.

It will also ensure our healthcare data is well protected, by mandating cyber and data security requirements for healthcare providers and third-party data intermediaries.

HealthierSG

The Health Information Bill (HIB) supports the safe collection and use of health info to promote better continuity of care by

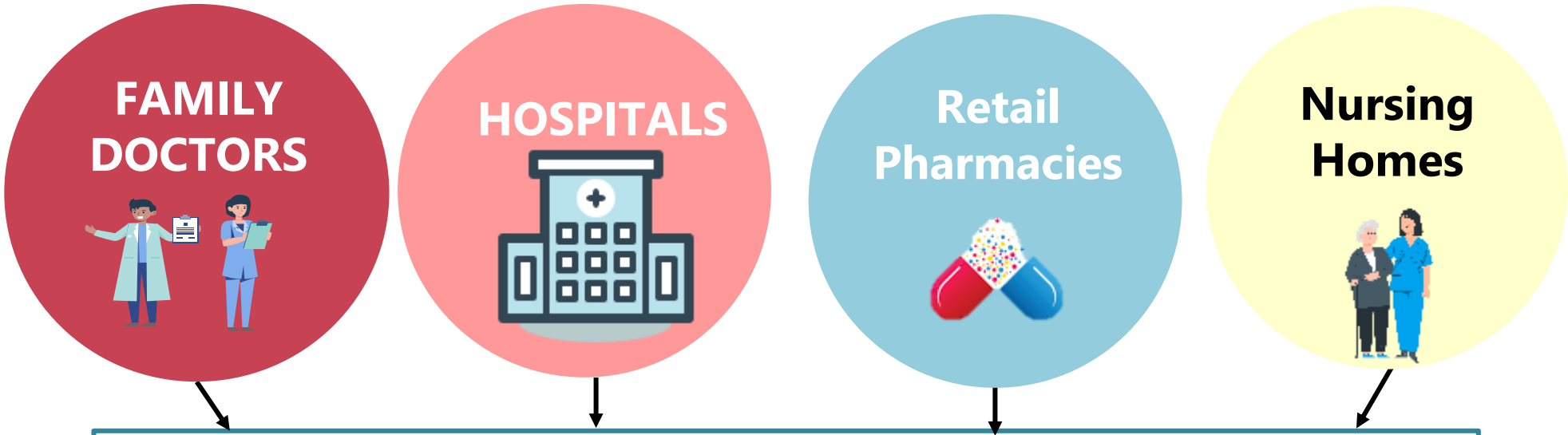
1. Building upon the current National Electronic Health Record (NEHR) repository, through mandatory contribution of selected key health information to NEHR by healthcare licensees *(e.g. hospitals, clinics, laboratories)* and extending access and/or contribution to prescribed users like retail pharmacists

2. Facilitating data sharing across MOH entities, private Healthcare Services Act (HCSA) licensees and appointed community partners

3. Ensuring safeguards for data sharing are in place to protect patient confidentiality and respect patient autonomy

4. Putting in place cybersecurity and data security measures to safeguard health information

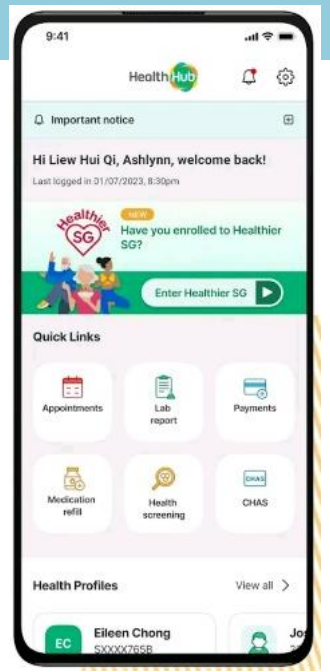
1. Mandatory contribution of selected health information to NEHR by healthcare providers



Provide a copy of selected health information in NEHR

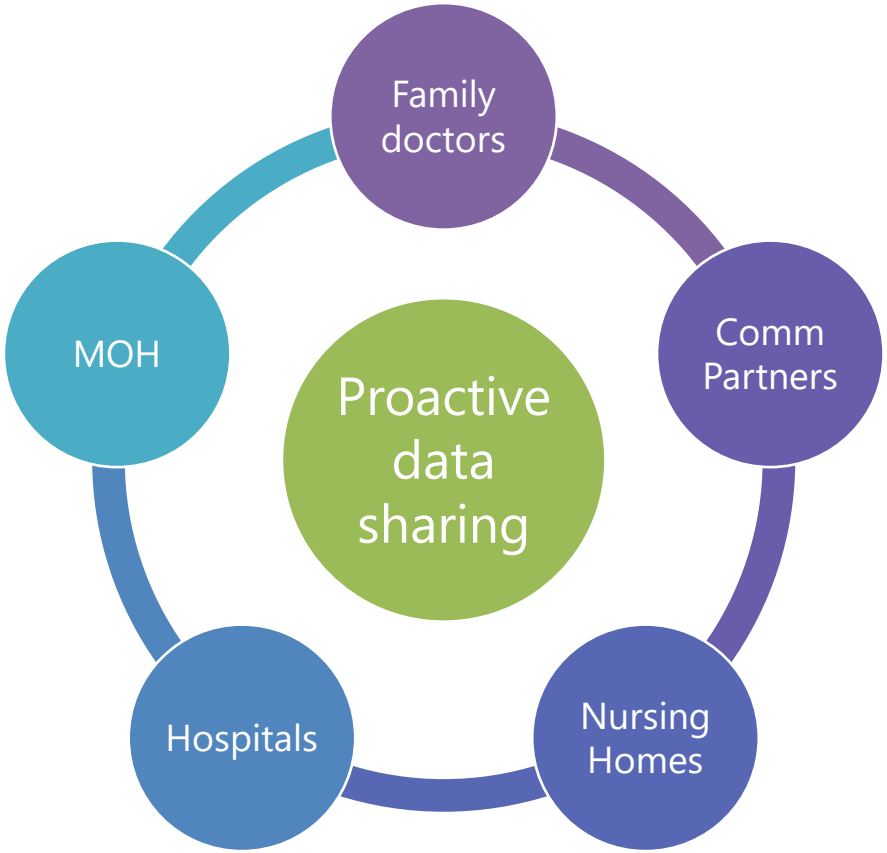
E.g. Demographics, Visit Diagnosis, Allergies, Procedure Notes, Investigation Results, Dental Charts, Prescribed Medications / Dispensed Medication, Discharge Summaries

- This ensures that healthcare providers involved in the patient's care journey would have access to up-to-date health information, including records from other providers, for more holistic care.



Residents/ patients may access their own selected NEHR data via HealthHub mobile app

2. Enabling Data sharing via Green Lane Provisions under HIB



Clinical data

✓Can leverage HIB to share between healthcare institutions and downstream to community for continuity of care purposes

X Cannot leverage HIB to share between community care partners

Administrative data

✓Can leverage HIB for MOH to share with healthcare clusters for outreach purposes

X Cannot leverage HIB to share between community care partners

Anonymised data

✓Shared conditionally by MOH

X Reidentification not allowed

Healthcare providers will be able to tap on HIB as the legal basis to share relevant administrative and clinical data with prescribed care providers and partners, for approved purposes such as continuity of care, eligibility for financial schemes and outreach, without prior patient consent.

3. Safeguards for health information sharing

- Patients can view in HealthHub Access Logs which institution has accessed their NEHR records
- Additional access control (double log-in) for healthcare professionals accessing Sensitive Health Information (SHI)

Guidelines for healthcare providers on appropriate access and use of health data in NEHR

Patient may place restrictions on NEHR access, and block data sharing by healthcare providers.

Access to NEHR prohibited for insurance and employment purposes (unless permitted by law)

4. Cybersecurity and data security measures to safeguard health information

Data intermediaries, such as providers of Clinic Management Systems, medical devices, and IT vendors, are also important stakeholders in the health information landscape.

Healthcare providers must meet cybersecurity and data security requirements for IT systems and medical devices

Data intermediaries will also be accountable if they fail to make reasonable arrangements to secure health information

Healthcare providers must report confirmed cybersecurity incidents and data breaches to MOH and notify affected individuals in a timely manner

Strict penalties will be imposed for any contraventions to the HIB requirements

Healthcare entities must meet a unified baseline set of cyber and data requirements

Cybersecurity

Update – *Software Updates*

- Install software updates on your devices and systems promptly.

Secure/Protect – *Virus/Malware Protection, Access Control, Secure Configuration*

- Use anti-malware and anti-virus solutions to protect against malicious software.
- Implement access control measures to control access to your data and services.
- Use secure settings for your organisation's procured hardware & software.

Backup – *Backup Data*

- Back up essential data and store them offline.

Asset – *People, Hardware & Software, Data*

- Equip staff with cyber-hygiene practices as the first line of defence.
- Identify the hardware and software used in your organisation, and protect them.
- Identify the types of data your organisation has, where they are stored, and secure them.

Data Security

Secure – *Storage, Reproduction, Conveyance Requirements*

- Store your health information securely to prevent unauthorised access.
- Do not reproduce copies of sensitive health information unless necessary.
- Transport health information properly to avoid unwanted data exposure.

Identify – *Data Security Classification, Marking Requirements*

- Know the information sensitivity levels of the data to apply appropriate safeguards.
- Differentiate data of varying information sensitivity levels by marking their classification.

Access – *Authorised Users*

- Restrict access to health information for valid and relevant purposes.

Cyber and data security requirements also take alignment from prevailing nation-wide standards

Common Cyber & Data Security Requirements

Outsourcing & Vendor Management

- Understand the responsibilities set between your organisation and vendor.

Incident Response

- Prepared to detect, respond, and recover from incidents.

Disposal Requirements

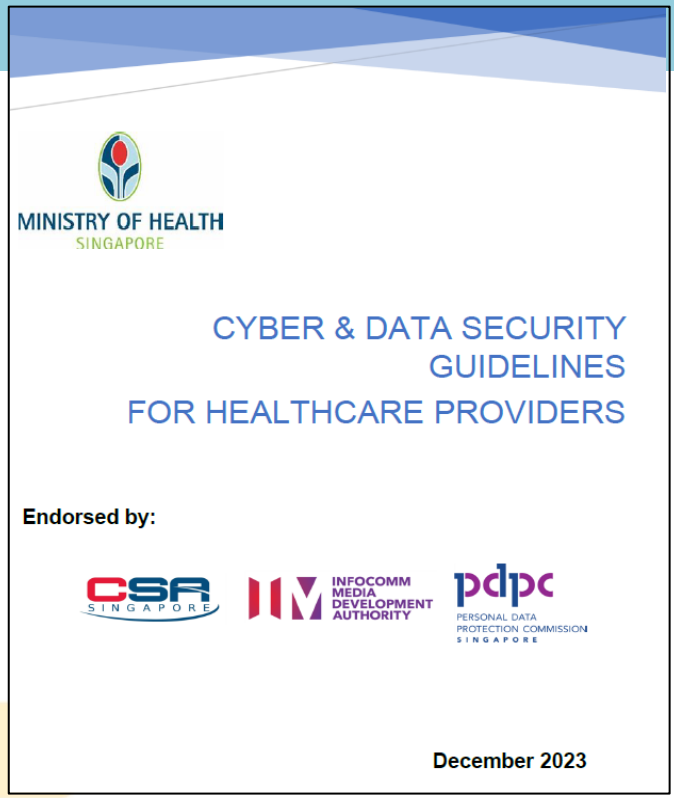
- Proper disposal of health information mitigates the risk of unauthorised access.

Emergency & Contingency Planning

- Supports ability to withstand service disruptions to ensure business continuity.

Review Security & Internal Audit

- Regular checks on corporate policies and processes to ensure compliance and identify vulnerabilities.



Unified set of cybersecurity and data security requirements

In tandem, we are developing professional guidelines on the appropriate use of the NEHR

Purpose

- Serve as a reference document for all healthcare professionals and illustrate **core guiding principles** on contribution to, and the access and use of NEHR in different clinical scenarios.
- **Address medicolegal concerns** raised by healthcare professionals by suggesting **reasonable professional standards that should be adopted** with regards to NEHR
- **Complements** the Bill, as well as professional ethical guidelines
- Will be **updated periodically** to reflect the changing healthcare landscape and evolving clinical practices

Content

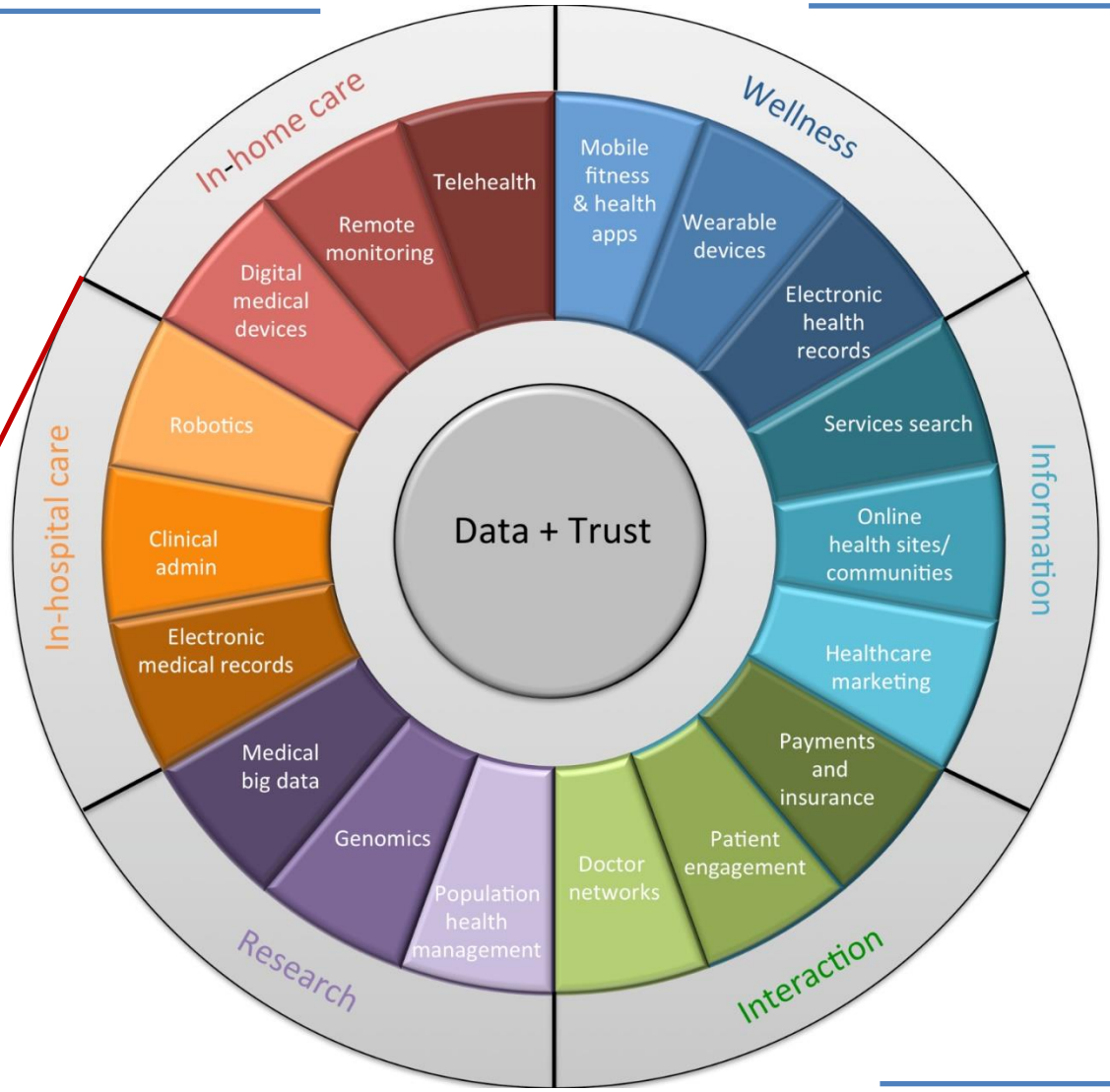
- Key Principles relating to a reasonable professional standard of care and conduct
  - *E.g., Healthcare professionals should ensure that they have sufficient reliable information about their patients before they offer any opinion, make management plans or treatment.*
- Guidelines on Contribution to NEHR
  - *E.g., Healthcare professionals should continue to make accurate, clear, and contemporaneous medical records as selected data will be made available on NEHR.*
- Appropriate Access to NEHR
  - *E.g., All information in NEHR should be treated with the same degree of confidentiality as other medical records.*
- Appropriate Use of NEHR
  - *E.g., Healthcare professionals should consider whether they have sufficient information before they decide if they need to use NEHR.*
- Scenarios to illustrate key guidelines

Proliferation of IoMT devices in Singapore

Healthier SG

1. Trusted care from family doctor
2. Focus on preventive health and healthier lifestyles
3. Empowerment to take charge of own health

1. Expansion of care provision to home and community services
2. Primary care to play a significant role
3. **Proliferation of devices to monitor and track health data remotely**



Source: STL Partners

Health Information Bill governing

1. Contribution of health information by healthcare providers
2. Sharing of health information
3. Autonomy of patients regarding their own data
4. Cybersecurity safeguards to protect the data

Cybersecurity incidents arising from IoMT devices are a matter of 'when', not 'if

Landscape of connected medical devices and cybersecurity concerns

- The global IoMT market size is predicted to grow **from USD30.79B in 2021 to USD187.60B in 2028***.
  - Greater connectivity and digitalization of medical devices has revolutionized the delivery of healthcare –
    - Improve efficiency, better disease monitoring and surveillance, lower care costs and drive better patient outcomes.
  - However, connection of devices to networks/internet brings about more cyber risks of medical devices
    - In 2022, **healthcare breaches** worldwide cost the most at about **USD10.10M**, compared to industry average of USD4.35M#

Examples of potential cyber risks of medical devices

Patient Safety

a) Alteration of medical information e.g. dosages on insulin pumps, images, test results

b) Modification of program or tampering of batteries resulting in malfunction e.g. on pacemakers, gastric stimulators

c) Ransomware causing denial of service e.g. failure of imaging equipment

Data Privacy

a) Exfiltration of data for public release or onto the dark web, cyber-espionage

b) Malicious activities spreading across corporate network, crippling the entire IT network of a hospital

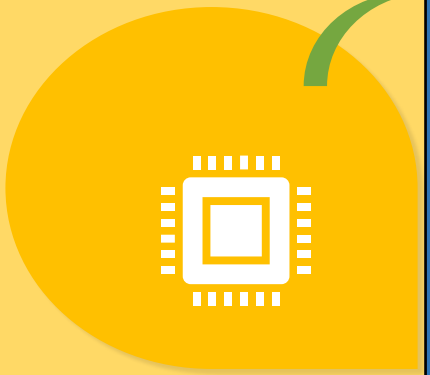
**Fortune Business Insights Oct'21; #IBM Security: Cost of a Data Breach Report 2022.*

Adopting a life-cycle approach to uplift the cybersecurity of Medical Devices

Pre-Market

Development & Market entry

- ❑ Promoting security-by-design
- ❑ Setting cybersecurity standards
- ❑ Supporting policies and regulations



Post-Market

Procurement

- ❑ Incorporating cybersecurity requirements into procurement process
- ❑ Compiling detailed inventory

Clinical Use

- ❑ Compliance to policy and standards for usage, maintenance, deployment, asset management & discovery, and decommissioning
- ❑ Ongoing risk assessment and treatment

Incident & Threat Detection and Management

- ❑ Developing real-time monitoring of MDOT network traffic and vulnerabilities
- ❑ Threat Management
- ❑ Incident reporting and management (detection, response and recovery)

Policy and Governance

- ❑ Developing cybersecurity policy, standards and guidelines for secure use through the lifecycle e.g. architecture, operating procedures etc.
- ❑ Promote awareness and culture, develop capabilities and build competencies, both in professional and consumer setting

Pre-market: Cybersecurity Labelling Scheme (Medical Devices)

Levels	Descriptions
1 +	Manufacturers need to meet the existing mandatory HSA requirements based on international standards adopted by major MD regulatory bodies (e.g. US FDA, Health Canada, Japan MHLW, TGA Australia) **&** Two additional cybersecurity requirements: Not using universal default password; and possessing anti-brute force mechanism.
2 ++	Manufacturers need to meet the enhanced security requirements titrated from MDS2, post-market policies and existing CLS standards.
3 +++	The software of the medical device (i.e., firmware, mobile applications, if available) undergo automated binary analysers to ensure no known critical software weakness, vulnerabilities or malware. **&** The device will also undergo a timebound penetration testing[(1)] to provide basic level of resistance against common cybersecurity attacks.
4 ++++	The software of the medical device (i.e., firmware, mobile applications if available) undergo automated binary analysers to ensure no known critical software weakness, vulnerabilities or malware. **&** The device will also undergo a timebound security evaluation[(2)] to provide higher level of resistance against cybersecurity attacks.

[(1)] *Penetration test: Evaluator performs testing using only limited information (i.e. only user guidance manuals that is provided with the device).*

[(2)] *Security evaluation: Evaluator is provided with information on the design/implementation of certain security functionalities (i.e. cryptographic functions). With more information, evaluator would be able to devise targeted tests and better assess the security functionalities of the device.*

Ongoing sandbox to implement CLS(MD)

SICW 2022

Announcement of the Cybersecurity Labelling Scheme for Medical Devices

Industry Consultation

January 2023

- **Publish of Industry Consultation Closing Note**
- **Manufacturers were invited to indicate their interest for the Sandbox**

August 2023

Launch of Sandbox

SICW 2023

~ Q4 2024 (TBC)

- **Launch of the CLS (MD)**
- **Successful Applicants from the Sandbox to be awarded the CLS(MD) label**

Sandbox Applications Summary

Updated On:	16 May 2024

Cybersecurity Labelling Scheme
FOR MEDICAL DEVICES
BY CYBER SECURITY AGENCY OF SINGAPORE

CLS(MD) Applications in pipeline	
Level 1	0
Level 2	4
Level 3	2
Level 4	0
Not Indicated	-

CLS(MD) Applications	
Submitted	34
Pipeline	6

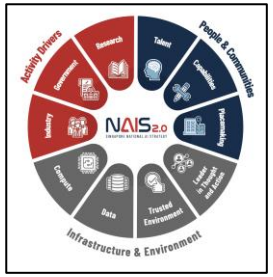
Submitted CLS(MD) Applications	
Level 1	14
Level 2	18
Level 3	1
Level 4	1

Singapore's approach towards regulating AI

- Singapore is committed to build a **trusted and responsible AI ecosystem** and adopts a **practical, risk-based approach** in AI governance to balance the need to protect public interests through safeguards and standards, while allowing maximal space for AI innovation for the public good.

National Guidance

Singapore National AI Strategy 2.0 (NAIS 2.0) (2023)

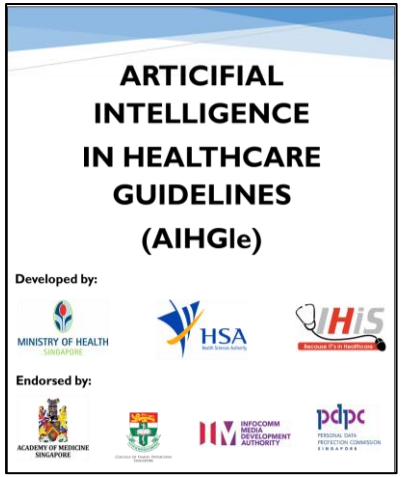


Model AI Governance Framework Second Edition (2020) for traditional AI

Model AI Governance Framework for Generative AI (in draft 2024)

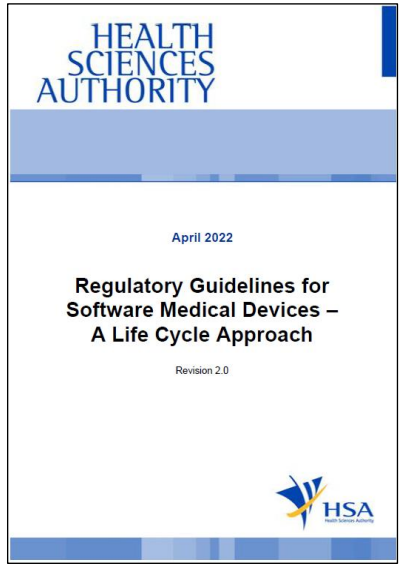
Healthcare Sector's Guidance

AIHGle (2021)



View AIHGle (PDF)

Regulatory Guidelines on AI-MD (2022)



BDAI in Human Biomedical Research (mid-2024)

In healthcare, AI is regulated by both MOH and the Health Sciences Authority

- **AI Medical Devices (AI-MDs) are regulated by our device regulator (Health Sciences Authority)**
- However there has been **no contextualized guidance on implementation risks.**

HSA Health Sciences Authority

MINISTRY OF HEALTH SINGAPORE

AI-MD

- AI-MD which treat, diagnose or manage care are regulated by HSA under the Health Products Act.
- HSA ensures the quality, safety and efficacy of AI medical devices

Risks

- Process
- Accountability
- Algorithm
- Data

Implementation

- **No contextualized guidance on how to implement and use AI-MD safely in healthcare**
- **Requires partnership between developers and implementers** to ensure safe deployment and risk mitigation.

HealthierSG

Supporting the safe growth of AI

Formation of the MOH AI Steering Committee (2024)

- **Better coordinate** efforts between MOH and key players in the healthcare sector for:
  - **AI Development & Adoption** – address co-ordination and support issues
  - **AI Governance** – address regulatory/practice related risks

AI Development & Adoption

- Identify and support public healthcare AI solutions from a pipeline of projects with **high-impact, relevance and effectiveness** for development and scaling through the MOH Healthcare Innovation (MHI) Fund.

AI Governance

- Provide guidance to promote **safe and responsible AI use** in healthcare and create an environment that **encourages innovation and expeditious adoption** of AI solutions.
  - 2 **Roundtables for AI Governance in the Healthcare Sector** (Apr and Aug 2024) – with Duke-NUS Centre for Regulatory Excellence
  - **Multi-stakeholder Working Group** under AISC to review AIHGle – includes regulators, public healthcare institutions, national healthtech; target stakeholder consultation by end-2024

DISCUSSION QUESTIONS

1) how is health information handled in your country – are there additional safeguards for sensitive health information such as abortion or mental health issues and how do you balance the need for patient privacy with need for sharing of information for care continuity?

2) Singapore plans to update our healthcare AI guidelines to address 3 main groups of stakeholders - product developers, implementors at the healthcare services/institutions, and individual healthcare professionals. How do we better manage and govern risks on use of AI across these three domains?

3) How do we support healthcare professionals to harness AI ethically and productively without compromising patient safety?

4) What are industry/healthcare institutions/clinicians' responses to the new compliance obligations arising from the EU AI Act?

5) How are consumers/patients involved in this effort to enhance their literacy in the proper use of healthcare AI tools?

Thank you

Contact us
Emma Zhang – Emma_ZHANG@moh.gov.sg