synapxe
Inspiring Tomorrow's Health

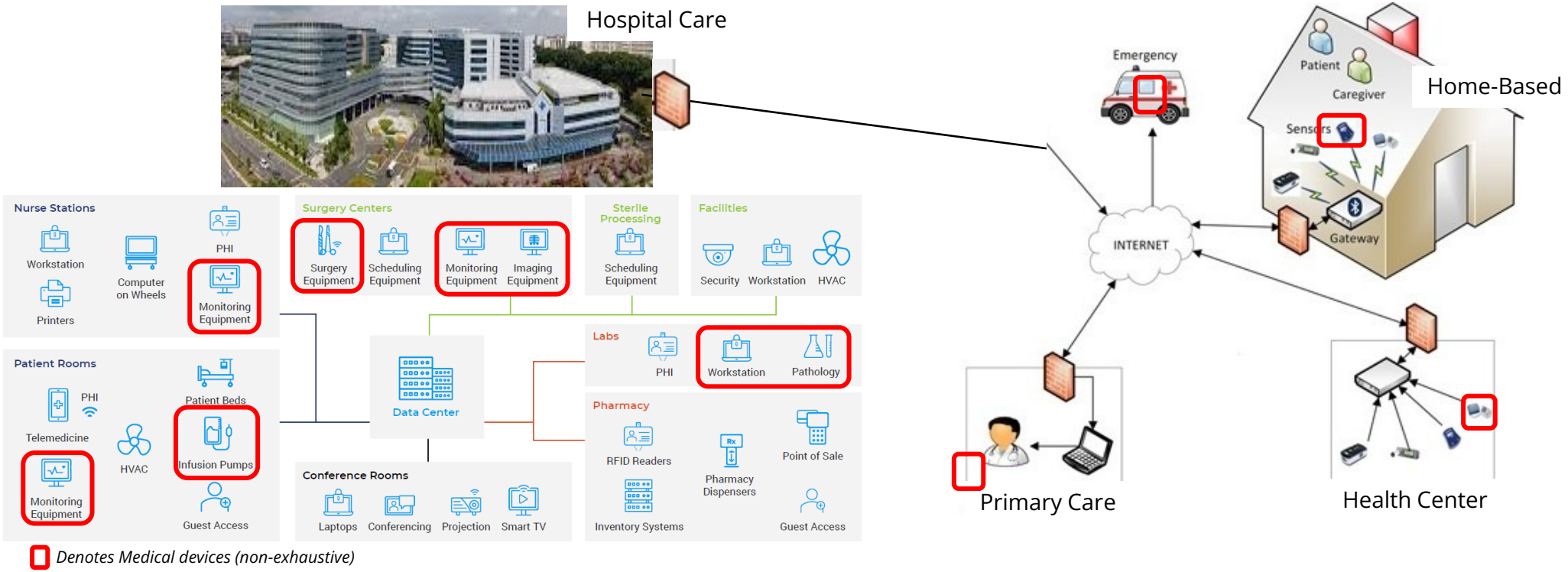
Uplifting Safety and Trust: Cybersecurity Labelling Scheme (Medical Devices), CLS(MD)

Mr. Devan Tay
Asst Director, Cyber Defence Group (Cap Dev.),
Medical Device Oversight Committee (MDOC) Program
Synapxe Pte. Ltd., Singapore

21 Feb 2025

Increasing connectedness in Healthcare delivery model

Connectivity and digitalisation of medical devices has revolutionised the delivery of healthcare.



Denotes Medical devices (non-exhaustive)

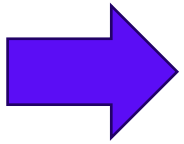
The global IoMT market size is predicted to grow **from USD30.8B in 2021 to USD187.6B in 2028***.

** Fortune Business Insights Oct'21*

Top 5 Healthcare Threats

Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP
CMS
HHS 405(d)



Social Engineering/ Phishing

Ransomware

Attack Against Connected Devices

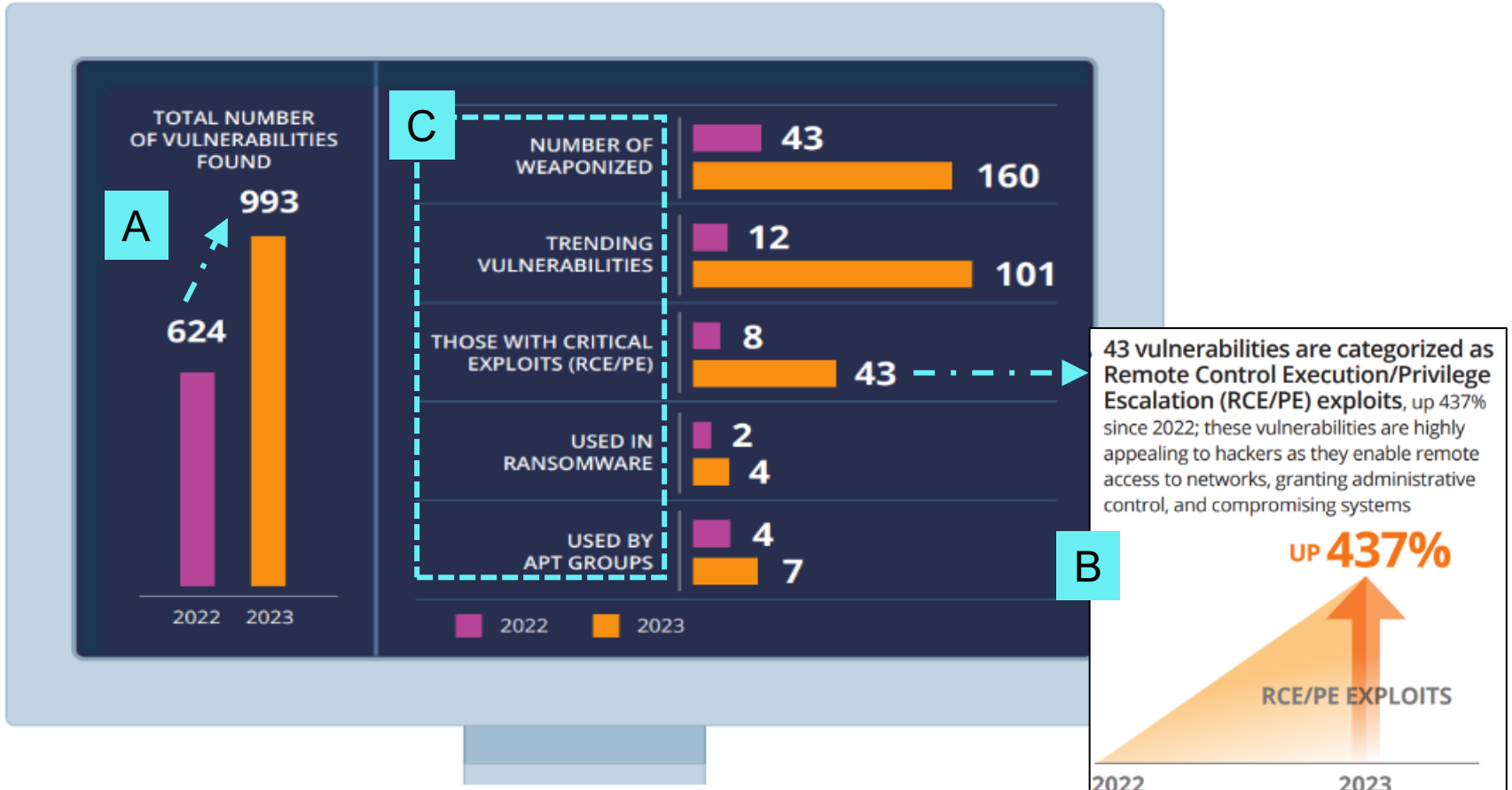
Loss or Theft of Equipment or Data

Insider Accidental or Malicious Data loss

https://405d.hhs.gov/cornerstone/hicp
https://405d.hhs.gov/Documents/405d-hospital-resiliency-analysis.pdf

Exploitable vulnerabilities in medical devices have increased

2023 State of Cybersecurity for Medical Devices and Healthcare Systems
(by H-ISAC, Securin, Finite State)



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

Contec CMS8000 vulnerability and threat alert

Contec CMS8000 vulnerability

Background:

- The Cybersecurity and Infrastructure Security Agency (CISA) has released information on a possible backdoor affecting the **Contec Health CMS8000 Patient Monitor (NCSC-25-01-031)** and its rebranded variant, the **Episemed MN-120**
  - Affected devices contain a hidden, unauthorised backdoor that has been intentionally programmed to connect to an IP address[#] registered to a University in Beijing, China.
  - The hard-coded IP address cannot be easily changed or disabled by users, leading to serious cybersecurity vulnerabilities ranging from high to critical severity* which could potentially allow attackers to carry out remote code execution, device modification, and to disrupt the devices' normal operations. The FDA further warned that this backdoor could compromise patient safety, disrupt hospital operations, and lead to regulatory repercussions for healthcare organisations.
  - Cybersecurity firm Claroty reported on 2 February 2025 that the IP address in question was documented in the Contec CMS8000 user manual for configuring the devices, indicating that it is a poor, insecure design flaw rather than a hidden backdoor for malicious purposes

**The vulnerabilities are: out-of-bounds write vulnerability (CVE-2024-12248, CVSS v4 score: 9.3), hidden functionality or backdoor (CVE-2025-0626, CVSS v4 score: 7.7) and privacy leakage (CVE-2025-0683, CVSS v4 score: 8.2).*

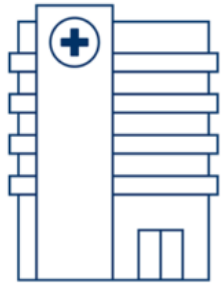
[#]Hard coded IP addresses: 202.114.4.119 and 202.114.4.120

Compromised medical devices pose serious risks

Patient Safety

Compromised medical devices can lead to misdiagnosis, improper treatment, and possibly loss of life.

Hospital Operations



Infected devices can cause systems to malfunction, ranging from life-saving medical devices to everyday hospital operation systems.

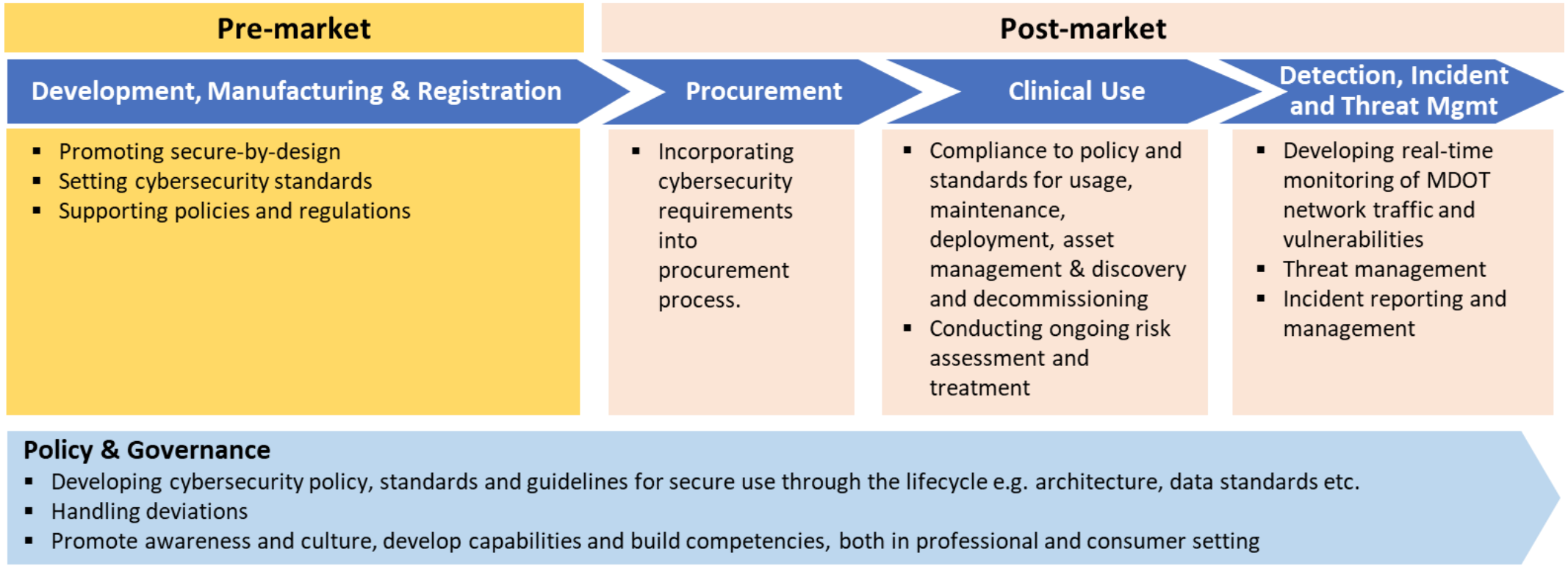
Data Confidentiality

Data breaches can lead to loss or exposure of patient data, compromising patient confidentiality and patient care.

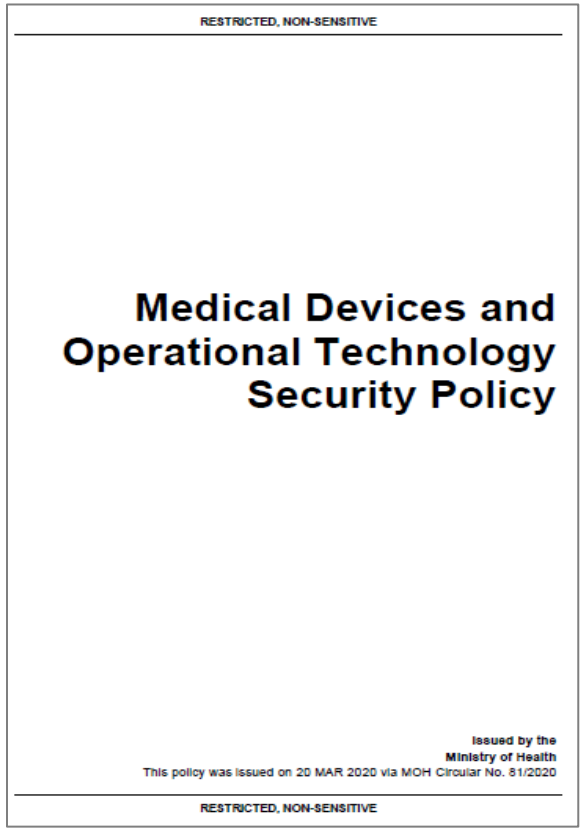
Medical Device Oversight Committee Program (MDOC)

Adopting a Life cycle approach to uplift the cybersecurity of Medical Devices

- Focusing to uplift pre-market capabilities, providing post-market diligence during procurement, securing clinical use, building detection, threat and incident handling capability as well as the development of policies, standards and governance.



Synapxe developed the Cybersecurity policy for public healthcare to comply for Medical Devices and Operational Technology


RESTRICTED, NON-SENSITIVE

Medical Devices and Operational Technology Security Policy

Issued by the
Ministry of Health
This policy was issued on 20 MAR 2020 via MOH Circular No. 81/2020

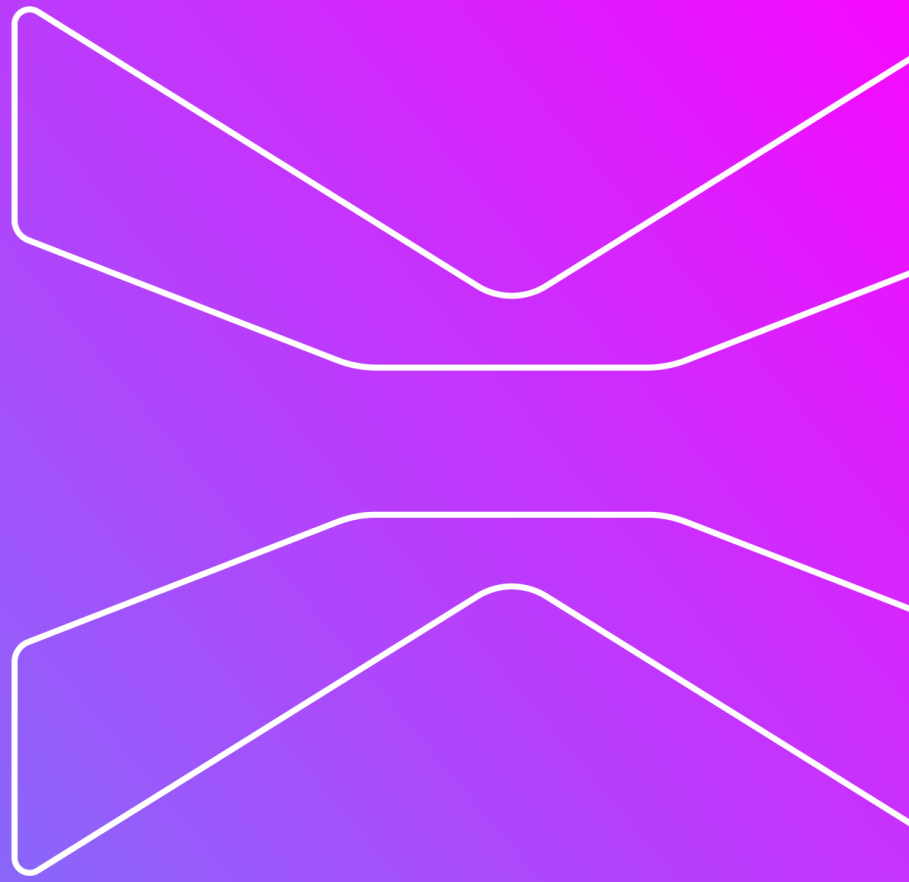
RESTRICTED, NON-SENSITIVE

History of Medical Devices and Operational Technology Security Policy (MDOTS)

- ❑ 20 Mar 2020: MOH Circular No. 82/2020 - Interim MDOTS policy
  - ✓ *5 measures + requirement for asset inventory*
- ❑ 29 Sep 2021: MOH Circular No. 136/2021
  - ✓ *Revised password requirements*
- ❑ 31 Aug 2023: MOH Circular No. 62/2023 - latest HIM-MDOTS policy
  - ✓ *Stepped up to 10 policy domains*
  - ✓ introduces additional requirements across five new domains, referencing industry standards and regulatory guidelines.

Successfully uplifted the cybersecurity baseline and awareness for Medical Devices and Operational Technologies in the public healthcare sector.

Cybersecurity Labelling Scheme for medical devices, CLS(MD)



CLS(MD) Journey

Pilot

Apr'22

SICW Oct'22

Announcement of the Cybersecurity Labelling Scheme for Medical Devices

Industry Consultation

Jan'23

Aug'23

Publish of Industry Consultation Closing Note

Sandbox launch

SICW Oct'23

Nov'23

Industry Sandbox Feedback session #1

Industry Sandbox Feedback session #2

Feb'24

Apr'24

Industry Sandbox Feedback session #3

End of Sandbox

20 July'24

SICW Oct'24

Launch of CLS(MD) Scheme


THE STRAITS TIMES

New cyber-security labelling scheme for medical devices in the works

The Cybersecurity Labelling Scheme for Medical Devices will assess the safety of healthcare equipment and certify

Cybersecurity Labelling Scheme (Medical Devices)

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

- Announced in Oct 2024, the CLS(MD) seeks to improve Medical Devices security, raise overall cyber hygiene levels and better secure Singapore's cyberspace.
- Medical devices that are in scope will be rated according to their level of cybersecurity provisions.
- This will enable consumers and healthcare providers to identify products with better cybersecurity provisions and make informed decisions.
- Incentivize manufacturers to develop more cyber-secure products.
- Consider nudges for market to use higher-level CLS(MD) devices in the near future.

Joint initiative between:

MINISTRY OF HEALTH SINGAPORE

CSA SINGAPORE

HSA Health Sciences Authority

synapxe
Inspiring Tomorrow's Health

In partnership with:

APACMed
The voice of MedTech

Singapore Manufacturing Federation 新加坡制造商总会

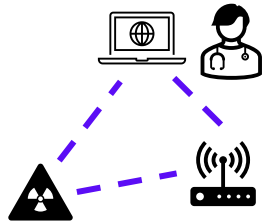
Medical Devices In-Scope for CLS(MD)

The CLS(MD) is a **voluntary scheme**.

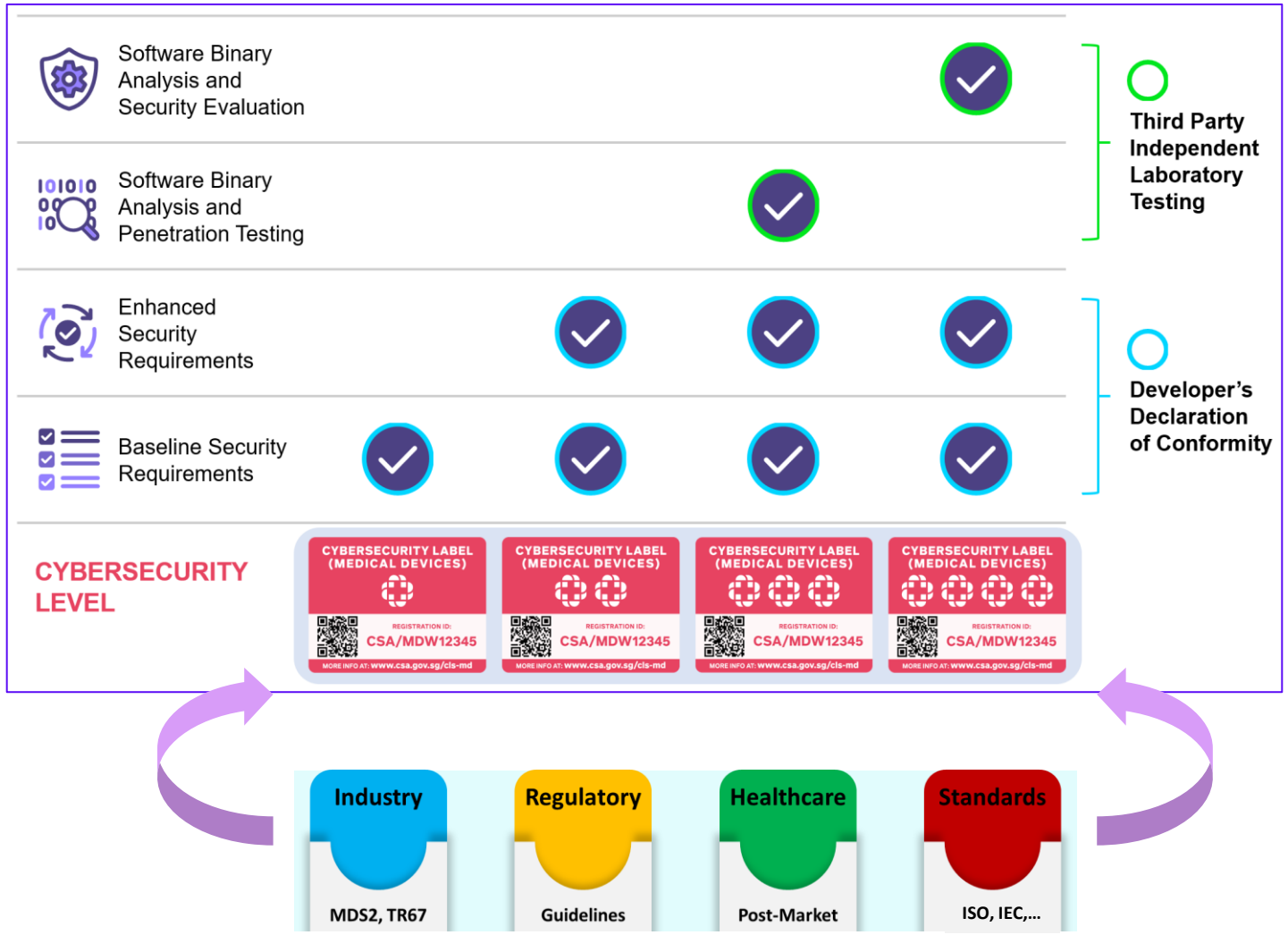
The scope of the CLS(MD) applies to **medical devices** as described in the First Schedule of the Health Product Act (Cap122D, 2008 Rev Ed) **and** have any of the following characteristics:

i. Handles personal identifiable information (PII) and clinical data and has the ability to collect, store, process, or transfer such data;

ii. Connects to other devices, systems, and services - Has the ability to communicate using wired and / or wireless communication protocols through a network of connections.



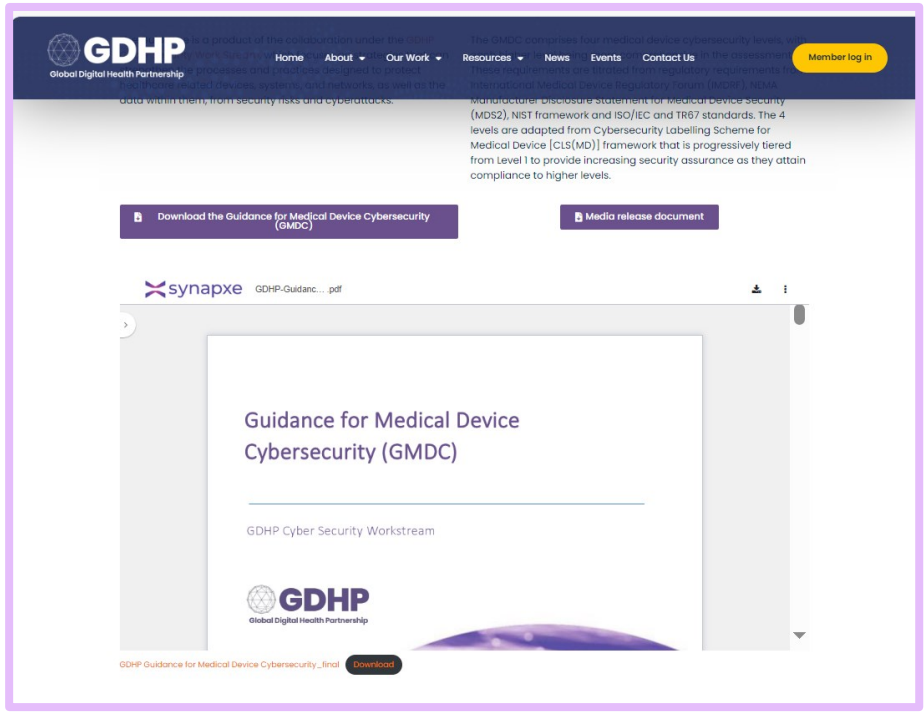
The CLS(MD) Framework



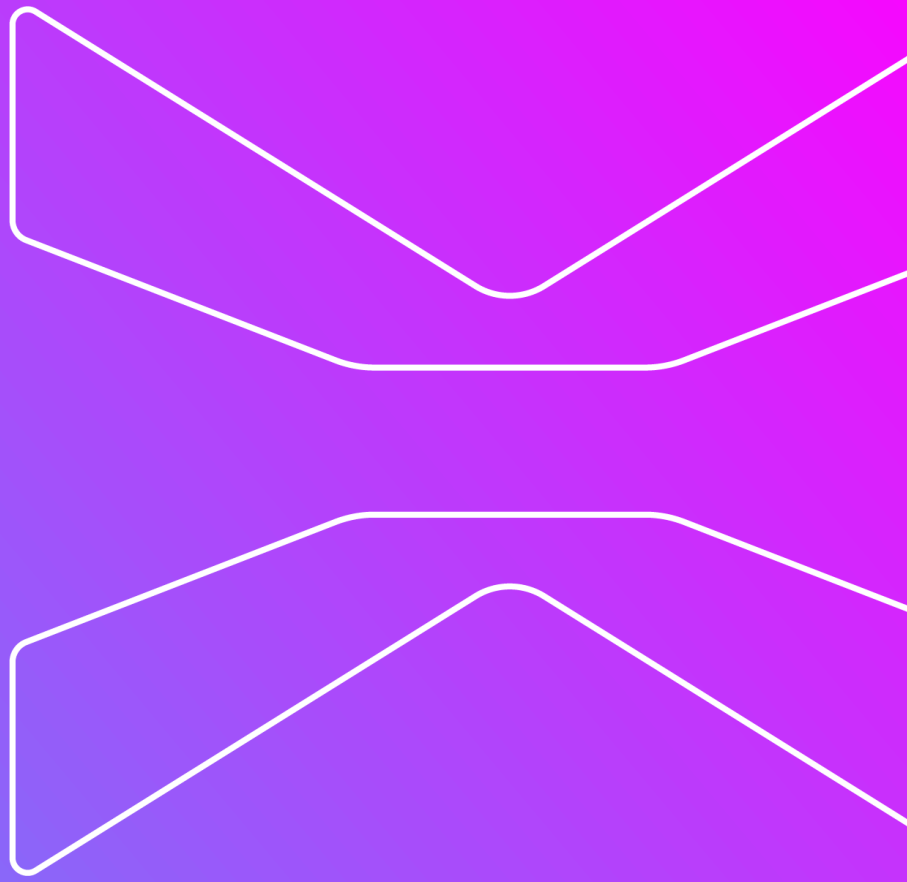
Levels	Descriptions
1	Manufacturers need to meet the existing 4 mandatory HSA requirements* based on international standards adopted by major MD regulatory bodies (e.g. US FDA, Health Canada, Japan MHLW, TGA Australia) **&** 2 additional requirements pertaining to No Universal default password and the need to possess anti-brute force mechanism.
2	Manufacturers need to meet the 32 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) to undergo automated binary analysers to ensure no known critical software weakness, vulnerabilities or malware. **&** The device is to undergo a timebound penetration testing to assure 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 is to undergo a timebound security evaluation to assure higher level of resistance against cybersecurity attacks.

Guidance on Medical Device Cybersecurity (GMDC) launched at GovWare on 16th Oct 2024, in collaboration with Global Digital Health Partnership to further CLS(MD) awareness globally

GMDC on GDHP website



Application Statistics

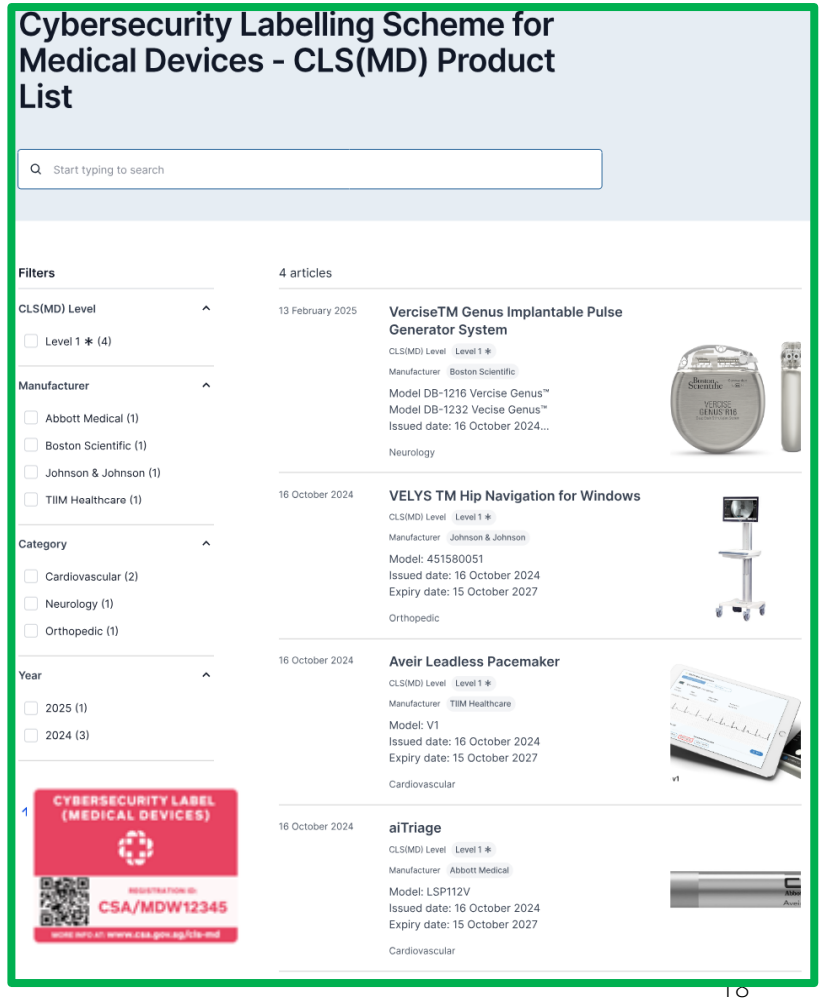


Application Statistics
- Overview of applications (as of 14 Feb 2025)

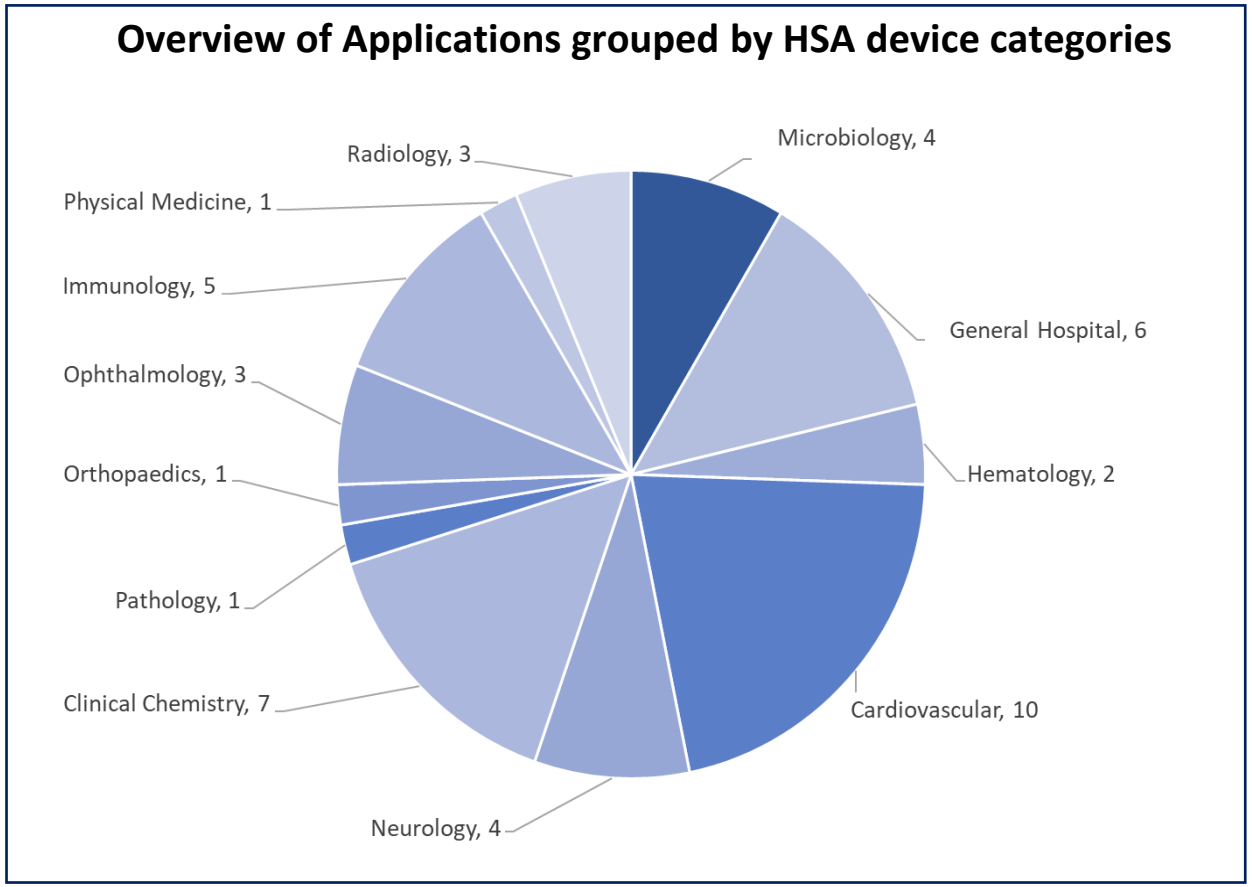
CLS(MD) Applications	
Submitted	49

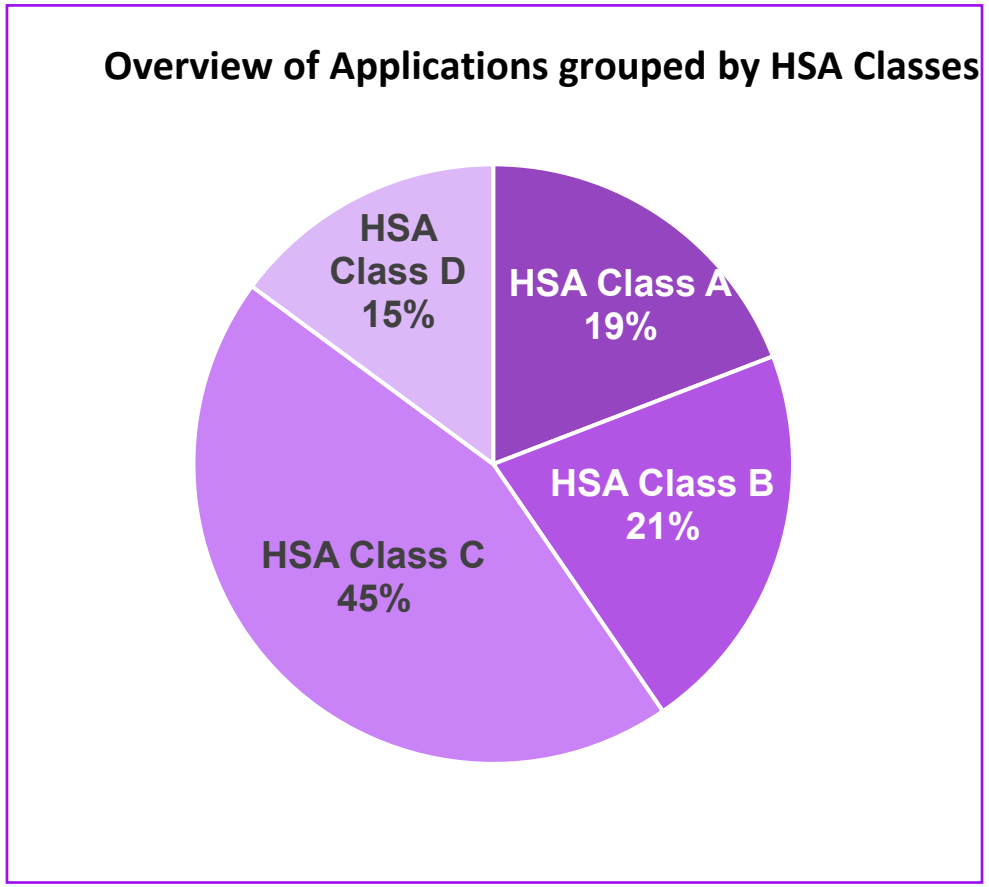
Submitted CLS(MD) Applications	
Level 1	14
Level 2	29
Level 3	5
Level 4	1

The following 5 devices have successfully attained Level 1.

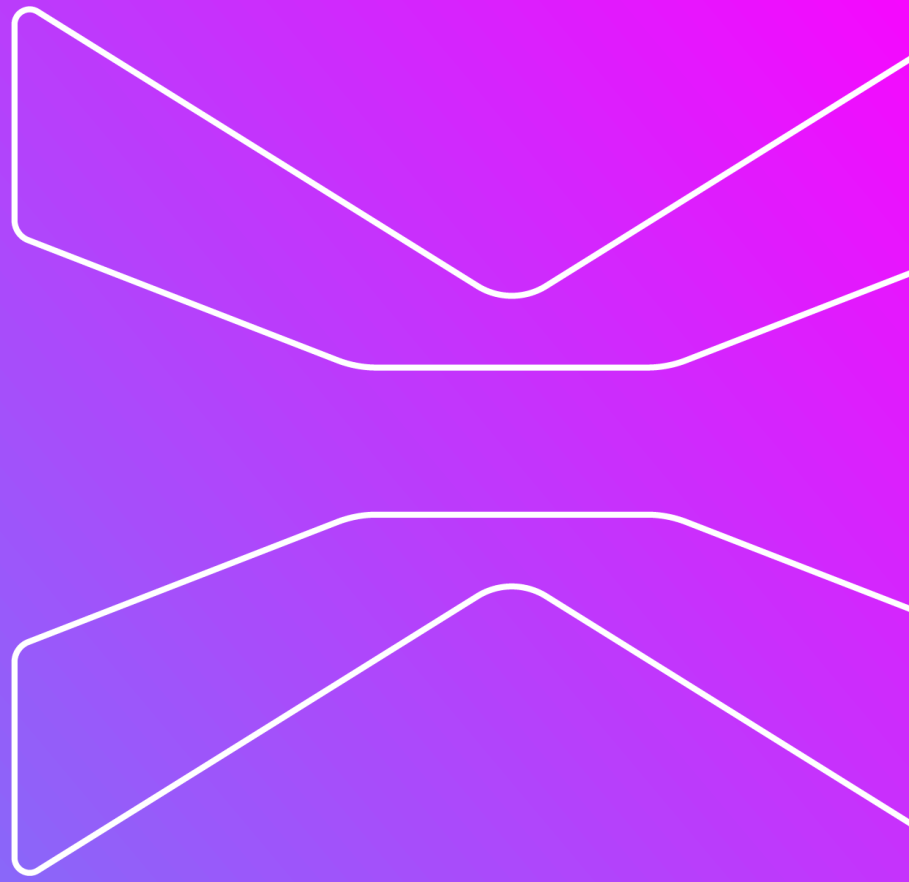


Application Status





Key Changes to the CLS(MD)



Declaration of Review to be Performed by Approved Test Laboratories

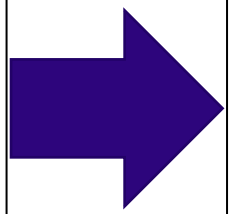
- For **new applications received from 16 October 2024**, manufacturers are required to engage an approved Test Laboratory (TL) for the review of the Declaration of Conformity (DoC) and Supporting Evidence (SE) before applying to the CLS(MD).

- For **applications (either in progress or waitlisted) received during the Sandbox**, the review of the Declaration of Conformity (DoC) and Supporting Evidence (SE) for levels 1 and 2 will continue to be reviewed by CSA.

Procedural Overview

Pre-Application Phase

1. Manufacturer will reach out to TL to establish terms of engagement and relevant non-disclosure agreements.
2. TL will perform the review of the manufacturer's DoC and SE.
3. When TL's review is complete, the CLS(MD) application can be submitted via GoBusiness Portal *(TLs may apply on behalf of manufacturers).*



Application Phase

1. The applicant shall submit the DoC, SE, and the TL's Assessment of the DoC/SE to CSA.
2. CSA will review the TL's assessment.
3. If the application is successful, CSA will proceed with label issuance.

Approved Test Laboratories

SG Healthcare Regulatory updates

To safeguard data and systems, a new Health Information Bill is proposed

The Health Information Bill (HIB) aims to ensure that <u>health information will be securely shared</u> across providers and care settings for holistic care and care continuity.

1. Building upon the current National Electronic Health Record (NEHR) repository, **mandate contribution of summary data** to NEHR by Healthcare Services Act (HCSA) licensees (e.g. hospitals, clinics, laboratories) and prescribe allowable uses of the repository

2. **Facilitate proactive data sharing** across MOH entities, HCSA licensees and appointed community partners

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

4. Put in place **cybersecurity and data protection measures** to safeguard health information

Cybersecurity and data governance measures to safeguard health information

Everyone must play their part in safeguarding health information

Healthcare providers and data intermediaries **must meet cybersecurity requirements and data governance measures** for IT systems and medical devices

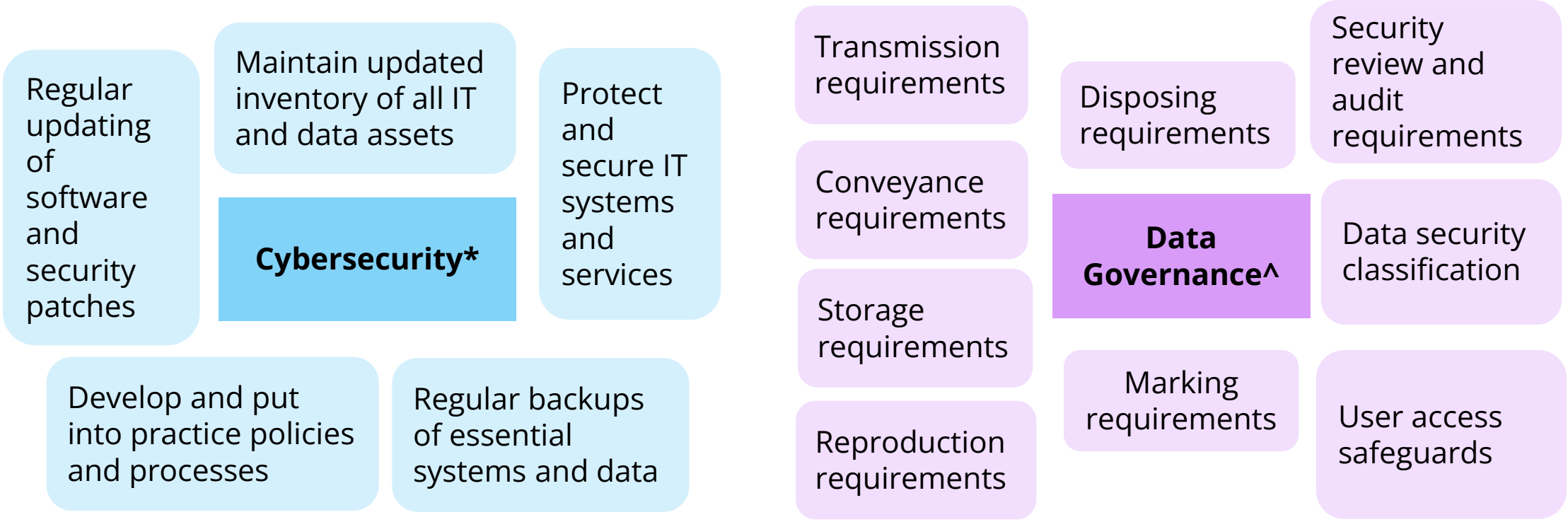
Healthcare providers must **report suspected cybersecurity incidents and data breaches** to MOH in a timely manner

Data intermediaries, such as providers of Clinic Management Systems and Medical Devices, are also important stakeholders in the health information landscape.

Data intermediaries will also **be held accountable** if they cause cyber / data breaches

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

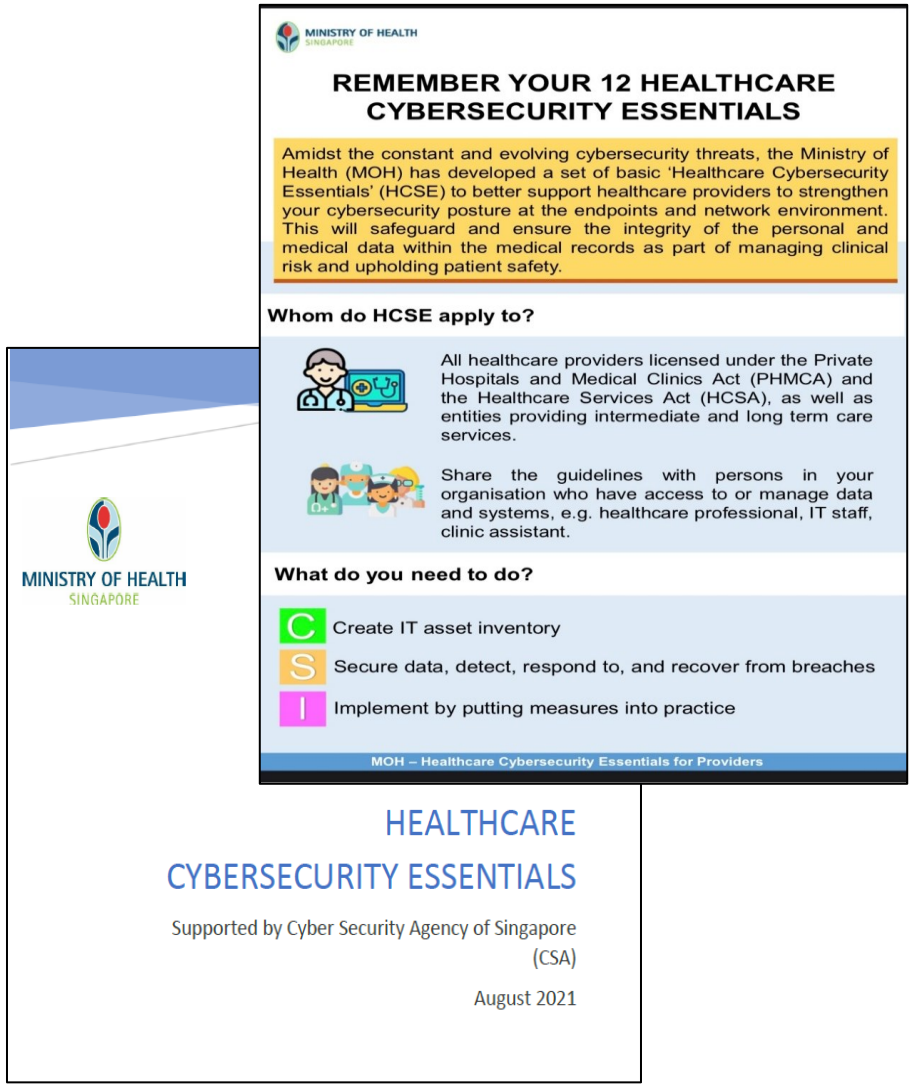
Healthcare entities must meet a unified set of baseline cyber & data requirements



*Builds on existing requirements under the **MOH Healthcare Cybersecurity Essentials (HCSE)**
^Aligned with prevailing PDPC **Personal Data Protection Act (PDPA)** standards

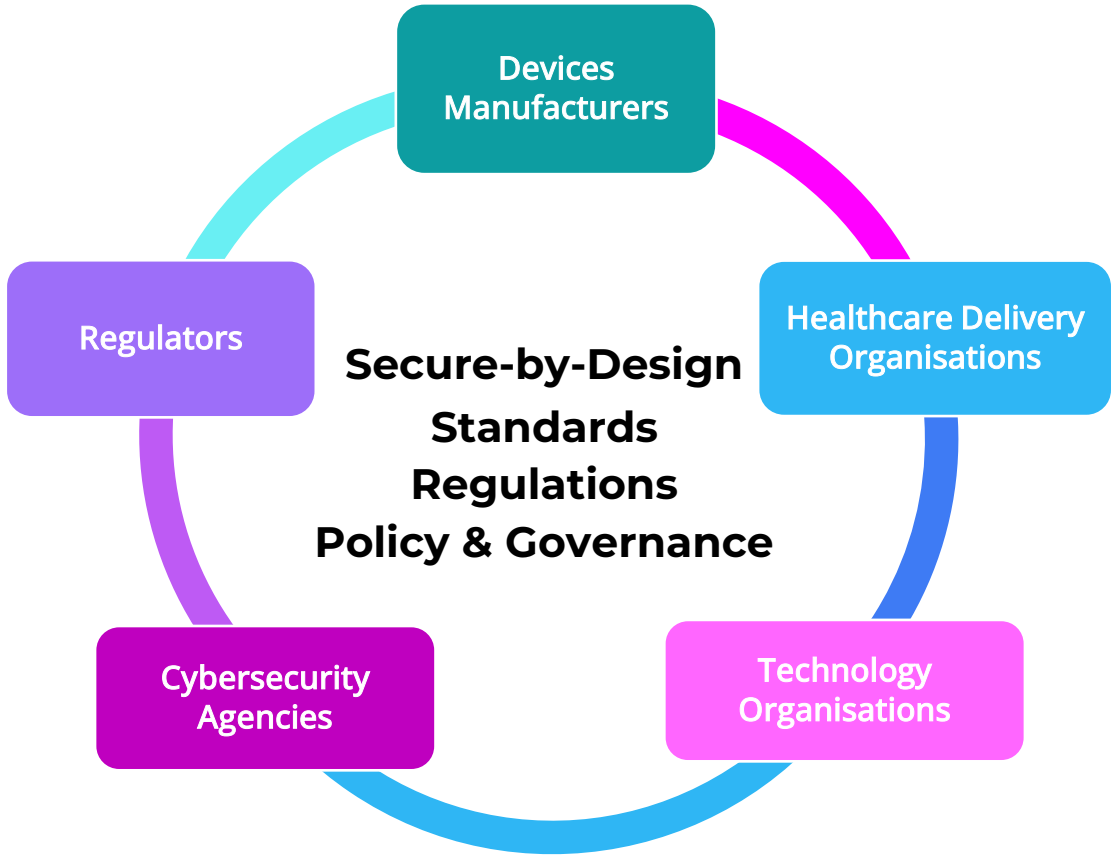
MOH Healthcare Cybersecurity Essentials (HCSE): an interim approach to ensure healthcare providers meet basic cybersecurity standards

- MOH (supported by CSA) developed and issued **Healthcare Cybersecurity Essentials (HCSE)**
  - Guide healthcare providers on basic cybersecurity measures.
- A **dedicated website** providing general information pertaining to cybersecurity was also set up
- **Consultations** are carried out as part of Health Information Bill (HIB) efforts on the cybersecurity standards required of medical devices, operational technology, and information and communications technology.



Call to Action: Collaborative Approach

Cybersecurity is a Team Sport…. Every member counts!



Multi-layered collaboration to Elevate the cybersecurity of medical devices

- Strong engagement of stakeholders
- Raise awareness and education
- Design and develop safer devices
- Regulatory and policy measures
- Balance cyber security and patient safety
- International Mutual Recognition

synapxe

Inspiring Tomorrow's Health

End of Presentation

THANK YOU

synapxe

synapxe

synapxe

synapxe.singapore

www.synapxe.sg