Regulatory Update for Health Sciences Authority, Singapore

Wong Woei Jiuang
Asst Group Director, Medical Devices Cluster
Health Sciences Authority, Singapore
March 12, 2024

IMDRF International Medical Device Regulators Forum

Facilitating SaMD Software Changes

- A new pathway for manufacturers to implement SaMD software changes, including AI related software changes, in a timely manner after device registration
- To establish confidence through good quality management practices, by demonstrating excellent capabilities in SaMD development, verification/validation, post-market surveillance/vigilance. Thus, proactively maintaining and improving the safety, efficacy and cybersecurity of their SaMDs
- Allow manufacturers to have better transparency and predictability in regulatory clearance for future software changes and facilitate faster implementation of significant software changes
- This initiative will be optional and can be enrolled through premarket registration process
- MDC will conduct industry consultation and focus group discussion to seek inputs and refine the approach

Line Extension Pathway

- A new pathway for line extension models to avoid duplicate review of previously reviewed data by HSA
  - Previous model must be registered with HSA
  - Line extension models are required to leverage on the same dataset as the previous model due to product similarity
- Potential to enhance the efficiency of the review process for line extension models
- This initiative is optional and can be enrolled through premarket registration process
- MDC will communicate to industry stakeholders on the details of the qualifying criteria at a later date

Cybersecurity Labelling Scheme for Medical Devices – CLS(MD)

Dr Alvin Lee
Deputy Director (Analytics & Capacity Building),
Aged & Ancillary Service Regulations & Transformation Division.
Ministry of Health Singapore

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

MINISTRY OF HEALTH SINGAPORE
HSA Health Sciences Authority
CSA SINGAPORE
synapxe Inspiring Tomorrow's Health

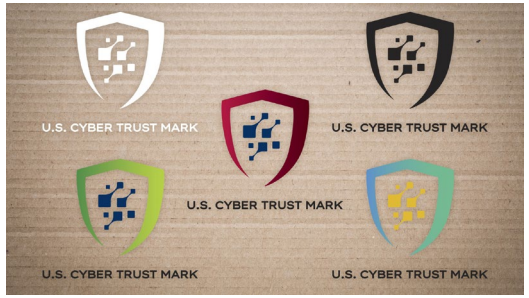
IMDRF International Medical Device Regulators Forum

Labelling schemes are not new…

IT

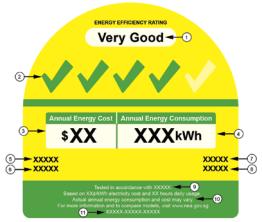
- US Cyber Trust Mark
- Australia's Smart Devices Cybersecurity Labelling Scheme
- Singapore's Cybersecurity Labelling Scheme

Cybersecurity Labelling Scheme
BY CYBER SECURITY AGENCY OF SINGAPORE



Non-IT

- Singapore
  - Water Efficiency Labelling Scheme (WELS)
  - Mandatory Energy Labelling Scheme (MELS)
  - Green Labelling Scheme
- Australia's Water Efficiency Labelling and Standards (WELS) Scheme
- Australia's and New Zealand's Equipment Energy Efficiency (E3) program



Burning platform – Patient safety at stake

CLASS I MEDICAL DEVICES	CLASS II MEDICAL DEVICES	CLASS III MEDICAL DEVICES
25 VULNERABILITIES	292 VULNERABILITIES	2 VULNERABILITIES

Home | Israel-Gaza war | War in Ukraine | Climate | Video | World | Asia | UK | Business | Tech

Tech

Home > In

NHS 'could have prevented' WannaCry ransomware attack

OPINION

Black Hat: Lethal Hack and wireless attack on insulin pumps to kill people

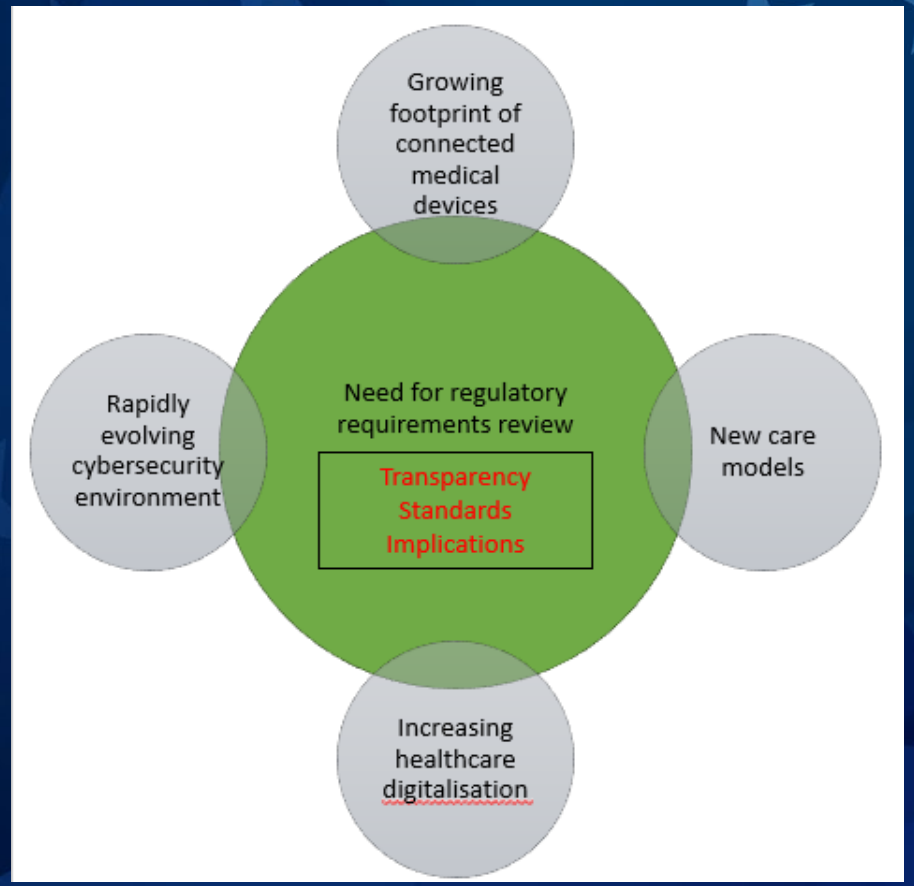
03/03/2020	SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices	The FDA is informing patients, health care providers, and manufacturers about the SweynTooth family of cybersecurity vulnerabilities, which may introduce risks for certain medical devices.
01/23/2020	Cybersecurity Vulnerabilities in Certain GE Healthcare Clinical Information Central Stations and Telemetry Servers	The FDA is raising awareness among health care providers and facility staff that cybersecurity vulnerabilities in certain GE Healthcare Clinical Information Central Stations and Telemetry Servers may introduce risks to patients while being monitored.
10/01/2019	Urgent/11 Cybersecurity Vulnerabilities May Introduce Risks During Use of Certain Medical Devices	The FDA is informing patients, health care providers and facility staff, and manufacturers about cybersecurity vulnerabilities for connected medical devices and health care networks that use certain communication software.
06/27/2019	Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks: FDA Safety Communication	The FDA has become aware of potential cybersecurity risks in certain Medtronic MiniMed Paradigm insulin pumps. The FDA recommends patients replace affected pumps with models that are better equipped to protect them from these potential risks.
03/21/2019	Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication	The FDA became aware of cybersecurity vulnerabilities identified in a wireless telemetry technology used for communication between Medtronic's implantable cardiac devices, clinic programmers, and home monitors. The FDA recommends that health care providers and patients continue to use these devices as intended and follow device labeling.

FDA U.S. FOOD & DRUG ADMINISTRATION

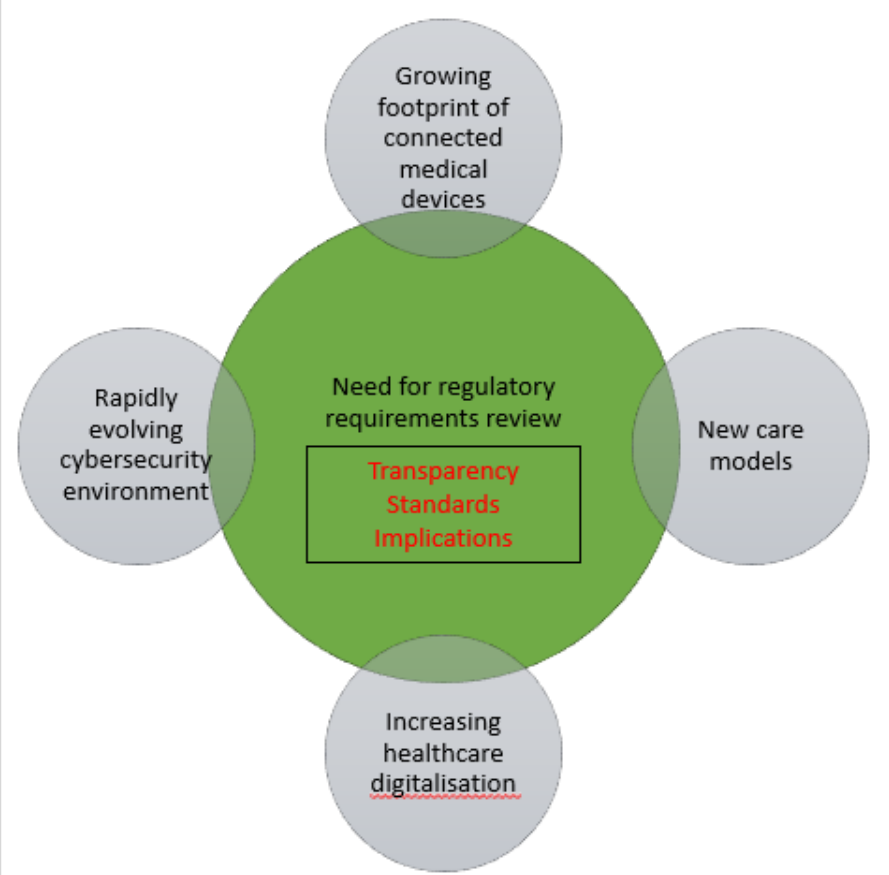
IMDRF 2024 Chair

IMDRF International Medical Device Regulators Forum

Burning platform – Patient safety at stake



Burning platform – Patient safety at stake



What the US Cyber Trust Mark Means for IoT Security in Healthcare

The US Cyber Trust Mark would provide consumers with cybersecurity assurances for smart devices and could have implications for healthcare in the future.

"Hopefully in the future, HDOs will be able to look to Cyber Trust Mark certification to identify and procure IoMT devices with stronger security, and in turn expand their fleets with more speed and confidence," Somasundaram added.

If adopted by a vote of the FCC, the US Cyber Trust Mark could be in operation as soon as late 2024. The Commission has already applied to register a national trademark for the US Cyber Trust Mark logo with the US Patent and Trademark Office.

Although the program will be voluntary, several major manufacturers and retailers have already made commitments to expand the program, including Google, Best Buy, Amazon, Logitech, LG Electronics USA, and Samsung.

Now, the FCC is seeking public input on key issues such as the scope of devices that should be eligible for inclusion in the labeling program, who should oversee the program, and how to establish and demonstrate compliance with security standards.

"Medical device manufacturers and [healthcare organizations] should also keep an ear to the ground on the specifics of government certification requirements as the US Cyber Trust Mark program and others develop," Somasundaram suggested.

Main Objectives

Consumers

1. Improve consumer safety
2. Empowered through transparency
3. Nudged towards important goals

Stakeholders Benefits

Regulators

1. Clear standards to uphold and enforce

Manufacturers

1. Improve standards of devices
2. Shared responsibilities

Scope of 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.

CLS(MD) framework – a collaboration among 4 agencies

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 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 to provide higher level of resistance against cybersecurity attacks.

CLS(MD) framework – a collaboration among 4 agencies

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 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 to provide higher level of resistance against cybersecurity attacks.

Sandbox

- **Started since October 2023 for nine months**
  - Finalise scheme requirements
  - Test operational workflow
- **36 devices committed with 19 applications submitted**
- **Provide labels at the end of the sandbox for successful devices**

Follow-up

- **Keen to work with IMDRF, or other regulators**
  - Share our experience and knowledge
  - Improve cybersecurity standards for connected medical devices
  - Discussion on how to adopt the standards within CLS(MD) into an equivalent ISO standard for MDs
- **More details of CLS(MD)** at www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cls-md

Questions


IMDRF
International Medical Device
Regulators Forum
United States
of America
2024