HEALTH SCIENCES AUTHORITY

December 2025

Regulatory Guidelines for Software Medical Devices including Machine Learning-Enabled Medical Devices – A Life Cycle Approach

Revision 4

HSA Health Sciences Authority

CONTENTS

1. INTRODUCTION 4
1.1 Objective 4
1.2 Intended Audience 4
1.3 Scope 4
1.4 Definitions 6
2. QUALITY MANAGEMENT SYSTEM (QMS) FOR SOFTWARE MEDICAL DEVICES 8
3. PRE-MARKET PRODUCT REGISTRATION REQUIREMENTS 10
3.1 Essential Principles for Safety and Performance of Medical Devices 10
3.2 Labelling Requirements 12
3.3 Software Versioning and Traceability 12
3.4 Design Verification & Validation 13
3.5 Clinical Evaluation 14
3.6 Risk Management 17
3.7 Cybersecurity 17
4. SOFTWARE MANUFACTURERS AND DISTRIBUTORS: ACTIVITY CONTROLS 19
5. CHANGES TO A REGISTERED SOFTWARE: CHANGE NOTIFICATION 20
6. POST-MARKET MANAGEMENT OF SOFTWARE MEDICAL DEVICES 23
6.1 Field Safety Corrective Actions (FSCA) 23
6.2 Adverse Events 25
7. SOFTWARE WITH MULTIPLE FUNCTIONS 25
8. CYBERSECURITY 26
8.1 Importance of Cybersecurity 26
8.2 Cybersecurity Considerations 26
8.2.1 Secure Device Design 27
8.2.2 Cyber Risk Management 28
8.2.3 Verification and Validation 29
8.2.4 Establishment of a post market management plan 30
8.2.5 Addressing Risks for Medical Device Operating System Reaching End of Support 31
8.3 Patient Confidentiality and Privacy and Other Regulations 32
9. MACHINE LEARNING-ENABLED MEDICAL DEVICES 32
9.1 Regulatory Requirements for MLMD 33
9.2 Additional Considerations for MLMD with Continuous Learning Capabilities 35
9.3 Post-market Monitoring of MLMD 37

9.4 Changes to Registered MLMD 37
10. Change Management Program (CMP) 40
11. REFERENCES 41

REVISION HISTORY

Guidelines Version (Effective Date) *[3 latest revisions]*	Revision
GL-04 SAMD – A Life Cycle Approach: First Release (30 April 2020)	R1
R2 ► GL-04: Revision 2 (29 April 2022)	R2
R3 ► GL-04: Revision 3 (01 March 2024)	R3
R4 GL-04: Revision 4 (31 December 2025)	R4

Changes and updates made in each document revision are annotated with or within the arrow symbol "►". Deletions may not be shown.

1. INTRODUCTION

Medical devices increasingly depend on software for safe operation and device interoperability. The rapid adoption of Artificial Intelligence (AI) and Internet of Things (IoT) in clinical settings introduces complex challenges (e.g., cybersecurity) for medical device software manufacturers.

To address this, all medical device software manufacturers should adopt a Total Product Life Cycle (TPLC) approach to manage rapid changes. This includes risk assessment, software verification and validation, change control, traceability, and continuous life cycle management.

1.1 Objective

The Health Sciences Authority (HSA) is issuing these guidelines to provide clarity on the regulatory requirements for software medical devices, including those with machine learning features, across the entire product life cycle. The requirements apply from product development through to post-market obligations for products supplied in Singapore.

1.2 Intended Audience

These guidelines are for stakeholders who develop or supply software medical devices in Singapore. Stakeholders may refer to https://www.hsa.gov.sg/medical-devices/guidance-documents for all referenced guidance documents.

1.3 Scope

These guidelines apply to software medical devices whose intended use meets the definition of a medical device under the Health Products Act 2007. This includes software medical devices which are intended for medical purposes such as investigating, detecting, diagnosing, monitoring, treating or managing any medical condition, disease, anatomy or physiological process.

This includes software supplied in the following forms:

Forms of Software	Examples
Software embedded in medical devices	• Diagnostic ultrasound imaging software • Software that delivers pacing or defibrillation in a pacemaker or ICD
Software that runs on general purpose computing platforms[1], including standalone medical mobile applications (also known as Software as a medical device (SaMD) in IMDRF context)	• Image processing software that runs on general purpose computing platforms • Mobile applications that remotely monitor a patient's vital signs • A web-based software that allows users to upload patient images for diagnostic purpose without installation on their computing device

Table 1: Description of the various forms of software medical devices

These guidelines apply to software medical devices in all risk classification and define regulatory requirements across the entire product life cycle. It includes key software-related regulatory requirements such as cybersecurity and requirements for Artificial Intelligence-enabled Medical Devices (AIMD) particularly those incorporating Machine Learning. These guidelines will also be reviewed and updated periodically to reflect emerging technologies and evolving risks

The following topics will be covered in this document:

- Quality Management System (QMS) for software medical devices
- Pre-market product registration requirements
- Dealer's licensing requirements
- Change notification
- Post-market management of software medical devices
- Cybersecurity
- Machine Learning-enabled Medical Devices (MLMD)
- Change Management Program (CMP)

[1] As per IMDRF/SaMD WG/N12FINAL:2014 Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations, "computing platforms" include hardware and software resources (e.g. operating system, processing hardware, storage, software libraries, displays, input devices, programming languages etc.)

1.4 Definitions

ARTIFICIAL INTELLIGENCE (AI): refers to a set of technologies that seek to simulate human traits such as knowledge, reasoning, problem-solving, perception, learning and planning. Based on the input it receives, AI generates outputs or decisions such as predictions, content, recommendations, and/or classifications.

ARTIFICIAL INTELLIGENCE-ENABLED MEDICAL DEVICE (AIMD): A medical device that uses artificial intelligence technology to achieve its intended medical purpose

CLINICAL EVALUATION: The assessment and analysis of clinical data pertaining to a medical device to verify the clinical safety and performance of the medical device when used as intended by the product owner.

COMPENSATING CONTROLS *(as defined in IMDRF/CYBER WG/70FINAL:2023)*: specific type of risk control measure deployed in lieu of, or in absence of, risk control measures implemented as part of the device's design (AAMI TIR97:2019).

CYBERSECURITY *(as defined in ISO 81001-1)*: a state where information and systems are protected from unauthorised activities such as access, use, disclosure, disruption, modification, or destruction to a degree that the related risks to confidentiality, integrity, and availability are maintained at an acceptable level throughout the life cycle

MACHINE LEARNING *(as defined in ISO/IEC 22989)*: process of optimising model parameters through computational techniques, such that the model's behaviour reflects the data or experience.

MACHINE LEARNING-ENABLED MEDICAL DEVICE (MLMD) *(as defined in IMDRF/AIMD WG/N67)*: A medical device that uses machine learning (ML), in part or in whole, to achieve its intended medical purpose.

MANUFACTURE *(as set out in the Act)*: in relation to a health product, means to make, fabricate, product or process the health product and includes: -

- any process carried out in the course of so making, fabricating, producing or processing the health product; and
- the packaging and labelling of the health product before it is supplied.

OFF-THE SHELF (OTS) or COMMERCIALLY-OFF-THE-SHELF (COTS) SOFTWARE: refers to pre-built and ready-made software usually from commercial supplier.

PRODUCT OWNER *(as set out in the Regulations):* in relation to a health product, means a person who:

- supplies the health product under his own name, or under any trade mark, design, trade name or other name or mark owned or controlled by him; and
- is responsible for designing, manufacturing, assembling, processing, labelling, packaging, refurbishing or modifying the health product, or for assigning to it a purpose, whether those tasks are performed by him or his behalf.

REGISTRANT *(as set out in the Act)*: in relation to a registered health product, means the person who applied for and obtained the registration of the health product under this *Act*.

STANDALONE MEDICAL MOBILE APPLICATION *(also known as SOFTWARE AS MEDICAL DEVICE (SaMD) in IMDRF context)*: a software and/or mobile application that is intended to function by itself and are not intended for use to control or affect the operation of other hardware medical devices.

2. QUALITY MANAGEMENT SYSTEM (QMS) FOR SOFTWARE MEDICAL DEVICES

All medical device manufacturers, including software medical device manufacturers, should maintain a QMS to ensure manufacturing quality. For software medical devices, good software quality and engineering practices are used to control product quality. The international standard: *ISO 13485 – Medical Devices – Quality Management Systems – Requirements for regulatory purposes*, specifies QMS requirements for organisation involved in any stages of the medical device life cycle.

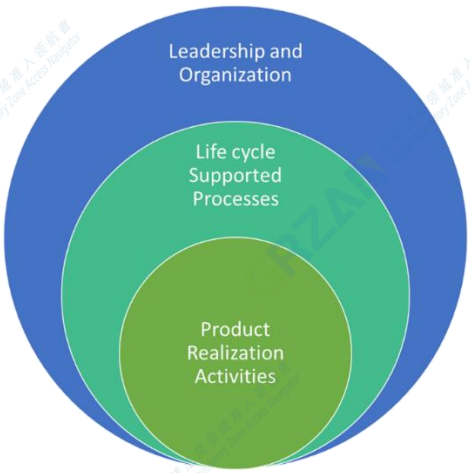


Figure 1: Quality Management Principles

An effective QMS for software medical device should include the following principles *(Figure 1)*:

- **Leadership and organisation:** Establish a clear organisational structure with accountable leadership to ensure management support and governance.
- **Life cycle supported processes:** Includes product planning, risk management, documentation and record control, configuration management and control, measurement, analysis and improvement, and outsource management should be applied throughout the software medical device product realisation activities.
- **Product realisation activities** that are commonly found in the software engineering life cycle approach are as follows:
    - Defining requirements
    - Design and Development

- Verification and Validation
- Deployment or Implementation
- Maintenance and Servicing
- Decommissioning

Please refer to *IMDRF/SaMD WG/N23 Final:2015 Software as a Medical Device (SaMD): Application of Quality Management System* and *ISO 13485 – Medical Devices – Quality Management Systems – Requirements for regulatory purposes* for more information on implementation of quality management system.

3. PRE-MARKET PRODUCT REGISTRATION REQUIREMENTS

Product registration applications for medical devices, including software medical devices, should be submitted to HSA in the ASEAN Common Submission Dossier Template (CSDT) format or International Medical Device Regulators Forum Table of Contents (IMDRF ToC).

Refer to the following guidance documents for information on CSDT format:

- *GN17: Guidance on Preparation of a Product Registration Submission for General Medical Devices using the ASEAN CSDT*
- *GN18: Guidance on Preparation of a Product Registration Submission for In Vitro Diagnostic (IVD) Medical Devices using the ASEAN CSDT.*

The mapping between the corresponding sections in the IMDRF ToC dossier and CSDT can be found in following documents:

- *E-Submission Guide for General Medical Devices for ASEAN CSDT and IMDRF ToC based Submissions.*
- *E-Submission Guide for IVD MD for ASEAN CSDT and IMDRF ToC based Submissions*

This section provides guidance on CSDT sections with software-specific requirements, including:

- Essential Principles for safety and performance of medical devices
- Labelling requirements
- Software versioning and traceability
- Design verification and validation
- Clinical Evaluation
- Risk Management
- Cybersecurity

3.1 Essential Principles for Safety and Performance of Medical Devices

All software medical devices, including Class A software medical devices, must be safe and perform as intended throughout their life cycle. Manufacturers should use the Essential Principles for Safety and Performance checklist (*GN-16: Guidance on*

Essential Principles for Safety and Performance of Medical Devices) to identify applicable design and manufacturing requirements for their software medical devices. Document the rationale for any requirements deemed not applicable. Table 2 lists the Essential Principles for Safety and Performance for software medical device.

Essential design and manufacturing principles	**Software embedded in medical devices**	**Software that can run on general purpose computing platforms, including SaMD**
Essential Principles applicable to medical devices and IVD medical devices		
General requirements	✓	✓
Clinical evaluation	✓	✓
Chemical, physical and biological properties	If applicable	
Sterility, packaging and microbial contamination	If applicable	
Considerations of environment and conditions of use	✓	✓
Requirements for active medical devices connected to or equipped with an energy source	✓	
Medical devices that incorporate software or are standalone software or mobile applications	✓	✓
Medical devices with a diagnostic or measuring function	✓	✓
Labelling and Instructions for use	✓	✓
Protection against electrical, mechanical and thermal risks	✓	
Protection against radiation	✓	
Protection against the risks posed by medical devices intended for use by lay persons	✓	✓
Medical devices incorporating materials of biological origin	If applicable	
Essential Principles applicable to medical devices other than IVD medical devices		
Particular Requirements for Implantable Medical Devices	✓	
Protection against the Risks Posed to the Patient or User by Medical Devices Supplying Energy or Substances	✓	
Medical Devices Incorporating a Substance Considered to be a Medicinal Product/Drug	✓	
Essential Principles applicable to IVD medical devices		
Performance Characteristics	✓	✓

Table 2: Essential design and manufacturing principles

3.2 Labelling Requirements

Device labelling (e.g. physical label, instructions for use) ensures safe and effective use of medical devices. It serves the following purposes:

- Identification: Provide essential information such as device name, software version, and product owner details to the user.
- Safety and performance: State intended purpose, proper use instruction, and safety warnings (e.g. contraindications).
- Traceability: Enable tracking of the device throughout its life cycle.

Software that is intended to run on general computing platforms, including SaMD, can be supplied in two ways: i) supplied in physical form or ii) supplied without a physical form. The table below outlines the minimum labelling requirements for each supply mode.

Supplied in physical form (i.e. CD/DVD)	**Supplied without any physical form (i.e. downloadable software, web-based software)**
Physical label and Instructions for Use (as per GN-23*: Guidance on Labelling for Medical Devices* for more information on labelling requirements for medical devices)	Provide a screenshot of the software's graphical interface (e.g. splash screen) showing identification elements, including the software version. Following information should be presented to user for software which are to be downloaded and installed by end user: • Internet address or web link to allow the end-user to download the software; and • The software download procedure; and • The software installation guide or procedure. These details ensure users can download and install the software correctly. Software must be traceable even though it has no physical form. There should be proper version control and access rights control to allow timely tracing of the software versions.

Table 3: Labelling requirements for the different forms of standalone software.

Please refer to *GN-23: Guidance on Labelling for Medical Devices* for more information on labelling requirements for medical devices.

3.3 Software Versioning and Traceability

Software versioning is essential for identification and post-market traceability in the event of software changes and field safety corrective actions. A description of the

software versioning and the traceability system implemented may be required during the registration process.

The registered software version in Singapore should be clearly indicated on:

- Device labelling if supplied in a physical form
- Software user interface if supplied without a physical form

Software version information on software changes/iteration (e.g. graphic interface, functionality, bug fixes) should be submitted. This does not include software version numbering that is solely for testing or internal use only (e.g. checking in of source code).

3.4 Design Verification & Validation

Software medical devices should be designed to be accurate, reliable, precise, safe, and effective for their intended use. Analytical validation should be performed to generate objective evidence of safety and performance, typically during the verification and validation (V&V) phase. Software verification ensures that design inputs produce the expected outputs, confirming the software meets its specifications. While software validation confirms the specifications meets user needs and intended use.

Software V&V reports should be provided together with the Software Requirement Specification (SRS). The SRS defines the functional, performance, interface, design, development, and other requirements. It serves as the baseline to confirm the software meets technical specifications and user needs.

Software V&V reports should include:

- Results of all verification, validation and tests performed before final release. The testing can either be performed in-house testing or in simulated user environments
- Objective evidence showing that specified requirements are met and that the software specifications met user needs and intended use.
- Any unresolved anomalies and deviations, with a documented assessment and justification for accepting them.

Reference to International Standards such as *IEC 62304: Medical device software – Software life cycle processes* is encouraged to demonstrate conformity to the essential requirements.

If the software version tested in validation reports differs from the version submitted for registration, provide a comparison of both versions and explain how the reports are applicable to the version to be registered. The need for specific validation to address significant differences between the two versions should be considered.

Provide traceability analysis (e.g. traceability matrix) that links product design requirements, design specifications, and testing requirement, and maps identified hazards to the implemented mitigations and their tests.

Medical devices are increasingly interconnected. When medical devices operate together or with other systems, manufacturers must address interoperability issues. Manufacturers must also implement measures to ensure safe, secure, and effective information transfer and utilisation among these medical devices and systems.

3.5 Clinical Evaluation

While software V&V confirms that the software medical device meets specified requirements and user needs, clinical evaluation demonstrates safety and effectiveness in the intended clinical setting.

The clinical evaluation process must establish a valid clinical association between the software's outputs and the target clinical condition for the stated intended use.

Clinical association measures how well the software's output aligns with real-world health conditions based on established scientific evidence and accepted clinical practices.

The clinical association can be substantiated by:

- Referencing existing literature and well-established clinical guidelines,

- Comparison with similarly established software medical devices on the market and/or,
- Conduct clinical studies for novel claims (e.g. new targeted population, new clinical condition)

In addition to establishing a valid clinical association, the software medical device should also be validated for its ability to generate accurate, reliable and precise output in the intended clinical environment, on the targeted patient population. Use measures such as sensitivity, specificity, and positive and negative predictive values in the clinical validation.

Table 4 summarises the type of clinical evidence recommended for software medical devices. The level of evidence required depends on how significant the software's output is (treat/diagnose, drive clinical management, or inform clinical management) and the state of healthcare situation or condition.

Device Characteristics	**Treat and Diagnose** Provide information that is the sole determinant to treat or to diagnose a disease or condition.	**Drive Clinical Management** Provide information for aid in treatment, aid in diagnosis, to triage or identify early signs of a disease or condition that will be used to guide next diagnostics or next treatment interventions.	**Inform Clinical Management** Provide information that is used in preventing/mitigating a disease or condition or to supplement clinical management of a disease or condition. Such information will not trigger an immediate or near term action.
Critical Situations or conditions where accurate and/or timely diagnosis or treatment action is vital to avoid death, long-term disability or other serious deterioration of health of an individual patient or to mitigating impact to public health.	• Literature Reviews • Clinical Experience • Clinical Studies	• Literature Reviews • Clinical Experience	• Literature Reviews • Clinical Experience

Serious Situations or conditions where accurate diagnosis or treatment is of vital importance to avoid unnecessary interventions (e.g. biopsy) or timely interventions are important to mitigate long term irreversible consequences on an individual patient's health condition or public health.	• Literature Reviews • Clinical Experience • Clinical Studies	• Literature Reviews • Clinical Experience	• Literature Reviews • Clinical Experience
Non-Serious Situations or conditions where an accurate diagnosis and treatment is important but not critical for interventions to mitigate long term irreversible consequences on an individual patient's health condition or public health.	• Literature Reviews • Clinical Experience • Clinical Studies	• Literature Reviews • Clinical Experience	• Literature Reviews • Clinical Experience

Table 4: Clinical evidence requirements for software medical device

For novel intended purposes or new target populations, manufacturers must provide clinical evidence (see Table 4) to establish the association between the software's outputs and the relevant clinical condition or physiological state.

Clinical evaluation is an on-going process throughout the software life cycle. After deployment, collect real-world data to confirm that the software continues to remain safe and effective. Continuous post-market monitoring allows manufacturer to:

- Detect new or evolving risks promptly
- Assess and update the risk–benefit assessment when needed
- Improve safety and performance through software updates (e.g. design changes) and labelling updates (e.g. limitations of use)

Please refer to *GN-20 Guidance on Clinical Evaluation* for more information on the presentation of clinical evidence for the purpose of product registration.

3.6 Risk Management

Manage risks across the entire software life cycle by identifying and addressing all foreseeable hazards and failure modes. Define the software's projected useful life and evaluate all risks, including cybersecurity vulnerabilities, to protect patients throughout use and as the software nears end of life. The level of risk assessment should match the software's complexity, risk class, and intended use.

Follow the principles described in "*ISO 14971 Medical Devices — Application of Risk Management to Medical Devices"*. Use a systematic risk management approach: (i) identify all possible hazards, (ii) assess the associated risks, (iii) implement mitigations or controls to reduce risks to an acceptable level and (iv) monitor and evaluate the effectiveness of mitigation measures.

For embedded software, evaluate the risk based on the medical device system, including the hardware components.

When software changes are made, systematically assess them for new or increased risks and implement additional risk controls as needed.

3.7 Cybersecurity

Implement the minimum necessary requirements concerning hardware, IT network characteristics, and IT security measures, including protection against unauthorised access, necessary to ensure the safe use of the software as intended. Submit the following information at product registration for software running on general purpose computing platform including SaMD or connected medical devices (e.g. with wireless features or internet-connected and network-connected functions):

i. Cybersecurity controls in place (e.g. design controls)
ii. Known and foreseeable cybersecurity vulnerabilities, risk analysis focusing on potential patient harm, and the mitigation measures implemented;
iii. On-going plans and processes to monitor, detect, and manage cybersecurity threats throughout the device's useful life, especially when a breach or vulnerability is detected in the post-market phase. This includes on-going plan that address cybersecurity concerns when the current operating system is reaching End of Support.

iv. Evidence that the security of the device/ effectiveness of the security controls has been verified. It should include the following, where applicable:
    - Descriptions of test methods, results, and conclusions,
    - A traceability matrix between security risks, security controls, and testing to verify those controls, and
    - References to any standards and internal SOPs/documentation used.

v. Details of the operating system (OS) the software medical device runs on, including the OS of the overall medical device system.

Reference to International Standards such as *IEC 81001-5-1: Health software and health IT systems safety, effectiveness and security* is encouraged to demonstrate conformity to the essential requirements.

Please refer to S*ection 8* for details on overall cybersecurity management for software medical devices.

4. SOFTWARE MANUFACTURERS AND DISTRIBUTORS: ACTIVITY CONTROLS

All dealers (manufacturers, importers, and wholesalers) of software medical devices should hold a medical device dealer's licence for each activity they perform. Licensing requires an appropriate QMS that:

- Ensures the software is developed and manufactured under an effective QMS (e.g. ISO 13485).
- Ensures traceability so software versions can be tracked to users (e.g. physicians or patients) in the event of a FSCAs or product defects.
- Ensures procedures are in place for post-market surveillance and response, including the ability to manage recalls and implement corrective actions (e.g. bug fixes, cyber alerts, patches) promptly and effectively, and to identify recurring issues.
- Maintains complete device records (e.g. customer complaints, distribution records, recall data) throughout the software life cycle.

Refer to *GN-02: Guidance on Licensing for Manufacturers, Importers and Wholesalers of Medical Devices* for further information on the requirements.

Table 5 presents HSA's current QMS and licensing requirements.

Note: Class B, C, and D software medical devices require product registration in all scenarios listed below.

Possible scenarios	**Requirements for supply to Healthcare Institutions or other licensed distributors**
i. Local entities that import and distribute software application in physical form (e.g. CD, USB and etc.)	• QMS based on ISO 13485 or SS 620 (GDPMDS) • Importer's and Wholesaler's licences
ii. Local entities authorised by overseas developers/product owners to provide or distribute software application through the internet or local online platforms (e.g. Apple App store, Google Play Store and etc.) for users to download and install the software application on their devices.	• QMS based on ISO 13485 or SS 620 (GDPMDS) • Importer's and Wholesaler's licences *Note: If the software application is supplied direct to general public, only Importer's licence is required*

iii.	Local entities that provide access to a cloud-based software application over the internet (typically via a web browser) without requiring installation on the user's device (e.g. for healthcare providers).	• QMS based on ISO 13485 or SS 620 (GDPMDS) • Wholesaler's licence
iv.	Local entities developing a software application locally, including design, programming, testing, and maintenance.	• QMS based on ISO 13485 • Manufacturer's licence *Note: Manufacturer's licence allows the manufacturer to distribute the software they manufacture*

Table 5: Licensing requirements for certain specific scenarios for software medical devices

5. CHANGES TO A REGISTERED SOFTWARE: CHANGE NOTIFICATION

HSA adopts a risk-based approach for changes to registered software medical devices, with requirements proportional to the significance of the change. Changes are classified into the following change categories depending on the impact and complexity of the change:

- Technical: Class C and D medical devices
- Review: Class B medical devices
- Notification: Class B, C, and D medical devices

Please refer to the flowcharts below (also found in *GN-21: Guidance on Change Notification for Registered Medical Devices*) to determine the change category (e.g. Technical, Review or Notification) for each software type (i.e. GMD, IVD).

When considering changes, evaluate both the software and non-software aspects of the registered medical device. Document all changes and keep them traceable within the QMS. All principles described in *GN-21: Guidance on Change Notification for Registered Medical Devices* will apply to software medical devices.

Changes to Software* of General Medical Devices (GMD)

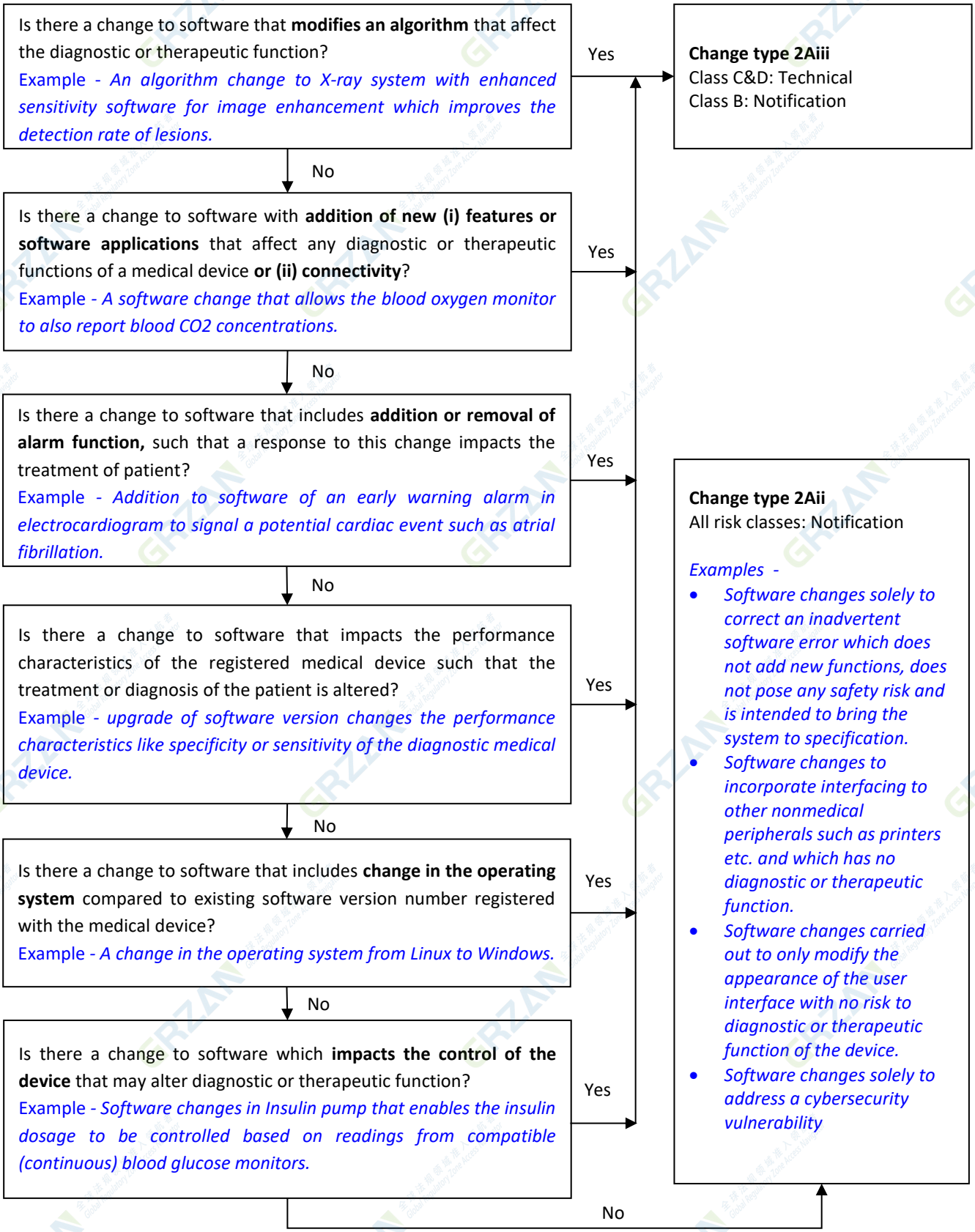


Figure 2: Flowchart for the changes to software of a GMD.
**Software refers to all software medical devices (e.g. SaMD, Software embedded in medical device system).*

Changes to Software of In Vitro Diagnostic (IVD) Medical Devices

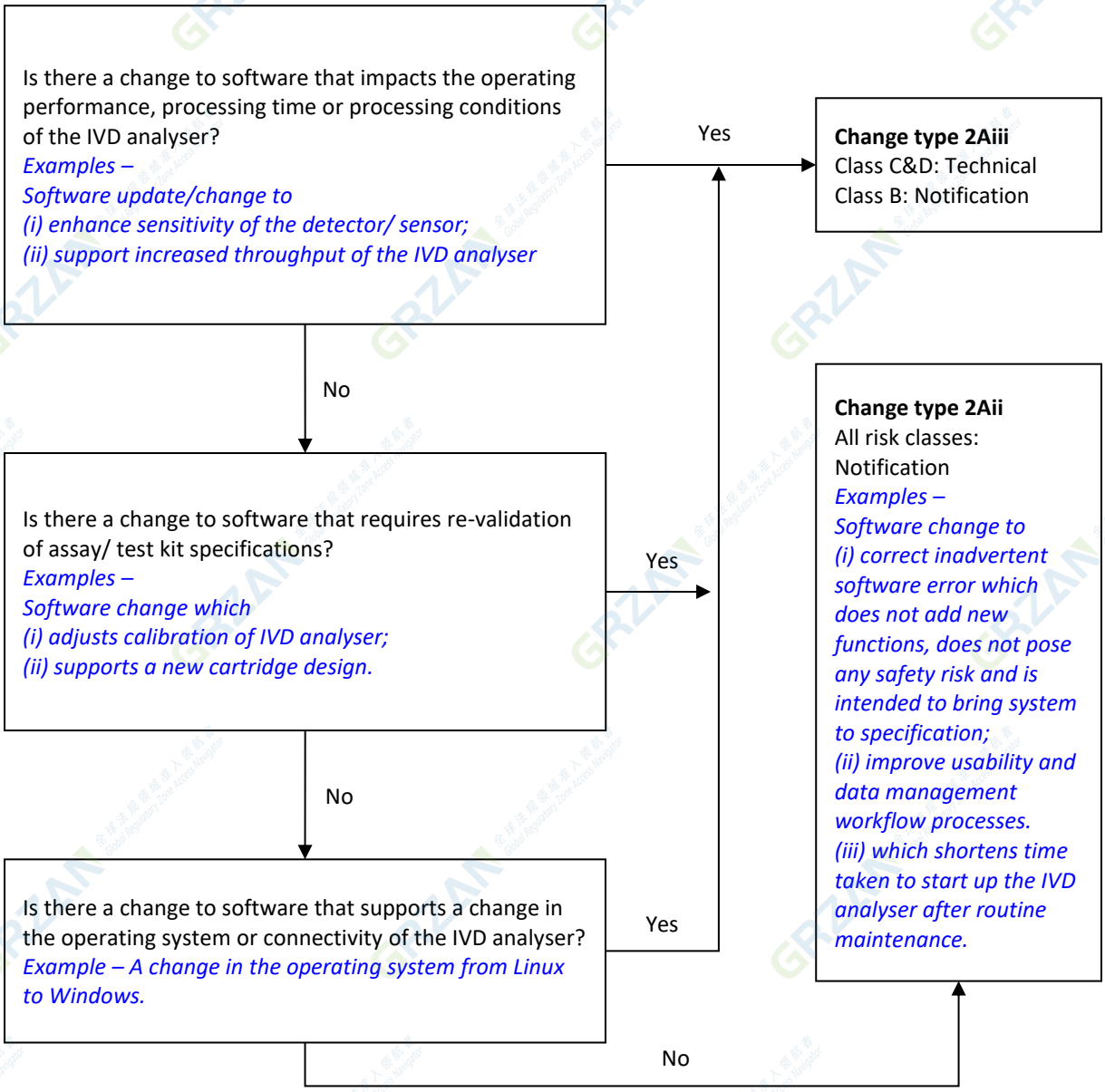


Figure 3: Flowchart for the changes to software of an IVD medical device.

6. POST-MARKET MANAGEMENT OF SOFTWARE MEDICAL DEVICES

Post-market monitoring and surveillance help detect software issues that may not appear during controlled development, validation, or clinical evaluation. Real-world use can introduce new risks due to diverse users, varying level of expertise, and different operating environments.

Dealers and registrants must fulfil post-market obligations, including reporting device defects or malfunctions, recalls and Field Safety Corrective Actions (FSCAs), and any serious injuries or deaths associated with the device.

This section provides an overview of post-market requirements applicable to software medical devices.

6.1 Field Safety Corrective Actions (FSCA)

Initiate a FSCA when it becomes necessary for the product owner of the medical device to take action (including recall of a medical device) to eliminate or reduce the risk of the hazards identified.

Common software medical device issues include the following (non-exhaustive list):

- Inaccurate or incorrect test results e.g. mixed up of patient results and demographics
- Failure to deliver therapy e.g. failure to deliver defibrillation in certain software modes
- Misdiagnosis and/or mistreatment e.g. uploading of incorrect treatment plan during exportation
- Calibration errors resulting in incorrect patient positioning
- Improper interface with external devices and/or other software components or modules e.g. with laboratory information systems (LIS)
- Incorrect image display e.g. flipped images when exported; display errors such as screen blank-outs or frozen screens
- Calculation errors e.g. software algorithm error resulting in wrong dose calculation for radiation therapy

- Configuration errors e.g. unit measurements not properly configured resulting in erroneous results reporting
- Alarm errors e.g. software bug causing incorrect alarm messages to be sent out
- Usability issues e.g. Graphical User Interface (GUI) related issues

Software errors or bugs can occur during design, development, or use of the device. Common causes of software errors:

- Incorrect, incomplete or inconsistent requirements and specifications
- Incomplete or lack of validation of software prior to initial release
- Not assessing the impact of changes during upgrades or bug fixes
- Misconfiguration e.g. failure to upgrade accompanying operating system
- Incompatibility with 3rd party installed program
- Poor interfacing with external devices or other software components/modules

Corrective and preventive actions typically involve bug fixes or software updates. Sometimes the software is not the cause (e.g. like a battery circuit fault reducing battery life) of the FSCA, but a software upgrade is required to reduce the risk (e.g. like adding an alarm to notify users when to change the battery after a set number of cycles).

When software medical devices need correction under FSCA, install the software upgrade or bug fix once available. Document the installed software version in service reports and keep these records for traceability.

For more information on FSCA reporting requirements, please refer to *GN-10: Guidance on Field Safety Corrective Action (FSCA) Reporting*.

6.2 Adverse Events

Adverse events (AE) involving software medical devices can directly or indirectly impact on patients and users. For example, insulin pump failures that affect blood sugar monitoring and insulin delivery may cause life-threatening hypoglycaemia. Software errors in IVD analysers can generate incorrect patient results, leading to misdiagnosis and inappropriate treatment.

Reports can originate from device log sheets, user complaints, and feedback. Manufacturers must investigate reports promptly and implement corrective and preventive actions to manage risks and prevent recurring adverse events.

AEs in software medical devices can be caused by many factors, including but not limited to:

- Software design flaws
- Inadequate verification and validation of the software code
- Inadequate instructions for use
- Software bugs introduced during implementation of new features

For more information on AE reporting requirements, please refer to *GN-05: Guidance on the Reporting of Adverse Events*.

7. SOFTWARE WITH MULTIPLE FUNCTIONS

Software medical devices often have multiple functions. Some functions do not meet the definition of a medical device under the Health Products Act 2007. Examples of non-medical-device functions are:

- Function that stores, converts, or transfers patient data
- Function that educates patients or facilitates access to commonly referenced information
- Function that automates general administrative operations (e.g. scheduling and billing) in a healthcare setting

Applicants do not need to submit information about non-MD functions during product registration. However, manufacturers must assess whether non-MD functions affect

device safety and performance (e.g. the clinical functionality is dependent on the non-MD function, device is vulnerable to cybersecurity attack due to the non-MD functions). Manufacturers must analyse and reduce these risks to acceptable levels through proper verification and validation. Document all risk management processes and actions as part of the QMS.

8. CYBERSECURITY

8.1 Importance of Cybersecurity

Cybersecurity is critical as medical devices become increasingly connected through wireless, internet, or other network connections. Cyberattacks can disrupt medical device availability and functionality, render hospital networks unavailable, and delay patient care. Security incidents threaten patient safety by causing diagnostic or therapeutic errors, compromising device performance, affecting clinical operations, or denying access to critical care.

Effective cybersecurity measures ensure software medical devices function safely. Manufacturers of software medical devices that communicate or connect with other systems must develop comprehensive cybersecurity strategies that address all possible risks throughout the device's useful life, not just during development.

Medical device cybersecurity is a shared responsibility among government agencies, manufacturers, healthcare institutions, and users. All stakeholders must work together to continuously monitor, assess, mitigate, communicate, and respond to cybersecurity risks and attacks throughout the device's life cycle. No single stakeholder can achieve effective cybersecurity alone.

8.2 Cybersecurity Considerations

Manufacturers must implement, maintain, and update a comprehensive cybersecurity plan throughout the TPLC covering development, support, limited support, and end-of-support phases (Figure 4).

Manufacturers should Include these considerations in the plan (non-exhaustive):

- Implement secure design principles to the device.
- Continuously identify, assess, and mitigate cybersecurity risks.

- Perform V&V testing to ensure security and functionality.
- Establish a post-market plan including ongoing surveillance, timely detection and response to emerging threats.
- Plan for and manage risks when the device's operating system is reaching end-of-support.

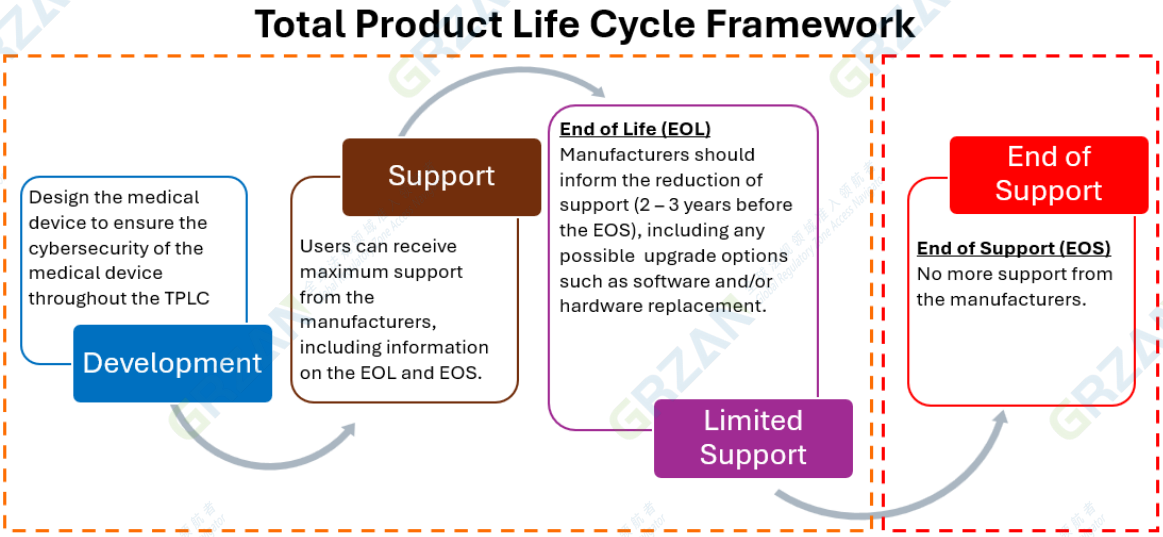


Figure 4: Total Product Life Cycle Framework from developer's perspective

8.2.1 Secure Device Design

Consider cybersecurity from the start of device design and development. Identify all possible cybersecurity hazards and include design features that secure the device. These features must prevent unauthorised use, detect security incidents and attacks, respond to cybersecurity threats, and recover from foreseeable cyber risks when possible.

Figure 5 shows some possible design considerations.

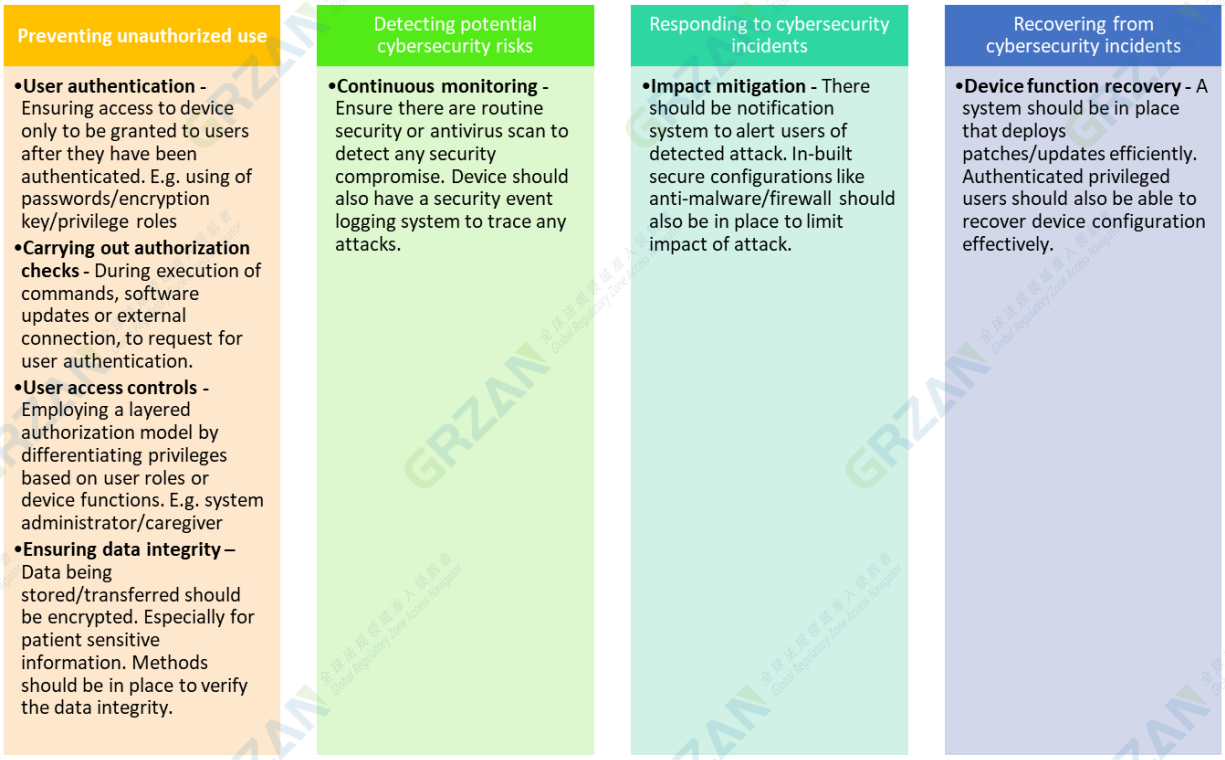


Figure 5: Cybersecurity design considerations (non-exhaustive)

8.2.2 Cyber Risk Management

Apply *ISO 14971 Medical devices — Application of risk management to medical devices* risk management to address medical device security and safety. Address cybersecurity risks that could compromise device safety and performance, disrupt clinical operations, or lead to diagnostic or therapeutic errors. Risk management must: (i) identify all possible cybersecurity hazards, (ii) assess the associated risks, (iii) implement mitigations to reduce risks to acceptable levels, (iv) monitor and evaluate mitigation effectiveness, and (v) communicate any residual risks to users.

Conduct and document this process consistently throughout the software life cycle. Map cybersecurity requirements to specific threats and vulnerabilities when they served as mitigation measures for the identified hazards.

Consider the following during the risk assessment:

- Use threat modelling tools to identify vulnerabilities and develop mitigations after evaluating the risks

- Cybersecurity and safety risk management should be conducted in parallel. When implementing security measures, consider overall patient safety to avoid

unintended harm. For example, requiring multi-factor authentication to access a Computed Tomography (CT) scanner could delay emergency use, so include an emergency bypass mode to maintain patient safety.

- When a new cybersecurity vulnerability is found, perform a risk assessment. This assessment should evaluate (i) the potential for patient harm, (ii) possible compromise of device performance, (iii) how easily the vulnerability can be exploited, and (iv) the severity of harm if exploited. Use a vulnerability scoring system to assess the exploitability and severity of cybersecurity vulnerabilities. Manufacturers can use established systems like the Common Vulnerability Scoring System (CVSS) or develop their own methods suited to their devices' specific risk profiles and operating environments. The assessment should also consider existing safety measures to determine if the cybersecurity risk is acceptable. If additional safety measures are needed, manufacturers must practise vulnerability disclosure to communicate effectively with all affected users and stakeholders. This information should include identification of affected devices, vulnerability impact, and available mitigations or compensating controls.

- Monitoring all software, including third-party software, for new vulnerabilities and risks that may affect device safety and performance.

- Implementing a process for timely detection and analysis of vulnerabilities and threats. This process should include impact assessment and follow-up actions such as threat containment, communication to affected parties, and vulnerability fixes.

8.2.3 Verification and Validation

Conduct comprehensive security testing to ensure code is free from significant known vulnerabilities and security controls are effectively implemented during verification and validation stage of design and development.

Security testing can include:

- Penetration testing
- Code analysis
- Vulnerability scanning
- Malware test

The device must maintain its intended functionality and essential performance even in the presence of residual cybersecurity risks.

8.2.4 Establishment of a post market management plan

Medical device systems are becoming more complex, and cybersecurity threats are evolving quickly. Healthcare networks are especially vulnerable because many devices are connected. Premarket controls alone cannot manage all cybersecurity risks. Manufacturers of software medical devices should implement a comprehensive, structured cybersecurity risk management plan throughout the software life cycle. As part of post-market management, they should actively monitor for threats and have a plan to detect and respond to new and emerging risks. Key considerations for this post-market plan include:

Post-market Vigilance	Establish a proactive plan to monitor, identify, assess and respond to newly discovered cybersecurity vulnerabilities throughout the device's useful life.
Vulnerability Disclosure	Establish a formal process to gather information from vulnerability finders, develop mitigation and remediation strategies, and disclose vulnerabilities and mitigation measures to stakeholders.
Patching and Updates	Create a plan which outlines how software will be updated to maintain ongoing safety and performance of the device, either regularly or in response to identified vulnerabilities. The plan should include processes to address concerns when the operating system approaches end-of-support (EOS).
Recovery	Create a recovery plan for the manufacturer, user, or both to restore the device to normal operating condition following a cybersecurity incident.
Information sharing	Involve in the communication and sharing of updated information about security threats and vulnerabilities, such as through Information Sharing Organisations (ISAOs), Information Sharing and Analysis Centres (ISACs).

Table 6: Cybersecurity post-market planning

8.2.5 Addressing Risks for Medical Device Operating System Reaching End of Support

When an operating system (OS) reaches End of Support (EOS), manufacturers must provide timely communication and adequate support to users before software medical devices reach EOS. This allows adequate planning for device retirement, alternative options, and business continuity.

The communication should clearly specify EOS dates, potential security risks, impact on device operation, and user responsibilities. Early planning and clear communication between manufacturers and users are essential to ensure patient safety and continuity of care when managing these medical devices in the market.

Software medical devices operating on unsupported OS with inherent cybersecurity risks that cannot be adequately mitigated are unacceptable and will not be permitted for supply in Singapore. The absence of security updates and vendor support after the EOS date can lead to new vulnerabilities that may compromise patient safety, data integrity, system reliability, and device performance, fundamentally undermining the device's safety profile throughout its life cycle.

Manufacturers must ensure that devices are equipped with current, supported OS that will remain viable throughout the device's intended lifespan. Device labelling must clearly state the OS requirements for software medical devices, particularly for software that runs on general purpose computing platforms, including SaMD. Unsupported OS must not be recommended in the labelling (e.g. IFU) unless adequate mitigation measures can be implemented to address security vulnerabilities effectively.

For existing deployed software medical devices running on unsupported OS, manufacturers must implement adequate mitigation measures to address cybersecurity risk associated with unsupported operating systems. These measures may include network isolation or update mechanisms to migrate systems to supported operating systems as per the company's ongoing plan in Sections 3.7 and 8.2.4.

Manufacturers must ensure that software medical devices undergo thorough compatibility assessment, including software V&V testing, when migrating to new supported OS. Where necessary, manufacturers must submit change notification applications as per *GN-21: Guidance on Change Notification for Registered Medical Devices*.

8.3 Patient Confidentiality and Privacy and Other Regulations

Medical device cybersecurity incidents can compromise patient safety and privacy. Data privacy breaches are increasing. Software medical device developers, implementers, and users must remain vigilant when handling confidential patient data and comply with local data protection and privacy legislation, such as the Personal Data Protection Commission (PDPC) 's Personal Data Protection Act (PDPA). Manufacturers and distributors are responsible for ensuring their medical devices meet all applicable regulatory requirements in Singapore.

9. MACHINE LEARNING-ENABLED MEDICAL DEVICES

Machine Learning (ML) is a subset of AI that includes deep learning (DL). ML develops models through algorithmic training on datasets. Unlike traditional medical devices with fixed algorithms, Machine Learning-enabled Medical Devices (MLMDs) improve their performance through training. This requires careful oversight in their development, validation, and ongoing monitoring to ensure patient safety and effectiveness.

MLMD follows the same regulatory principles as other software medical devices but presents additional challenges that need to be addressed, such as continuous learning capabilities, level of human intervention, model training, and retraining.

This section presents additional regulatory considerations specifically for medical devices that use ML. These ML specific requirements address the unique characteristics and challenges posed by ML algorithms in medical devices.

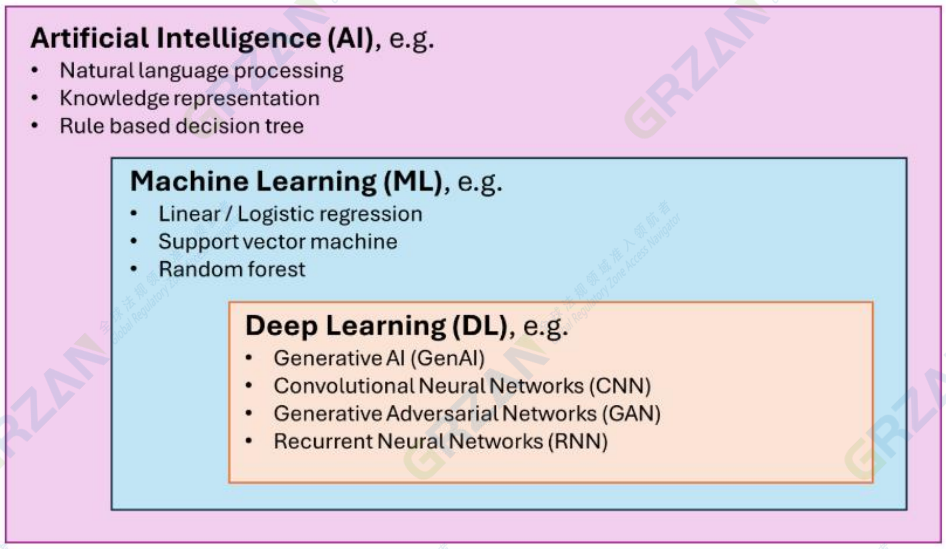


Figure 6: Relationship between AI, ML and DL

9.1 Regulatory Requirements for MLMD

All activities related to the design, development, training, validation, retraining and deployment of MLMD must be performed and managed under an ISO 13485 based quality management system (QMS). Refer to Section 2 in this document for further information.

The block diagram below illustrates the process of developing and deploying the MLMD.

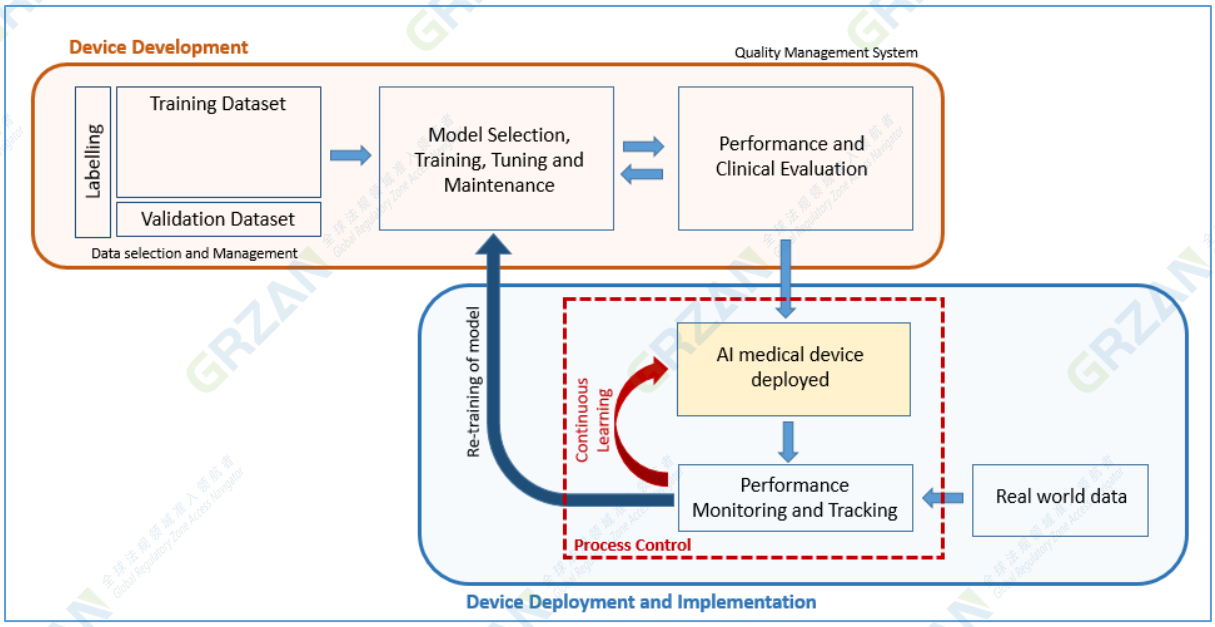


Figure 7: Typical illustration of a ML model

The following additional information should be submitted for pre-market registration of MLMD.

Requirements	Description
	Preclinical
MLMD Description	• Intended use and Indication for Use of the MLMD. • Description of the ML feature, including the clinical association between machine learning output and clinical condition(s).
End user communication	In addition to the labelling requirement stated under Section 3.2, clearly indicate the following information to the users: • Intended use and indication for use of the MLMD. • A statement informing users that the device contains ML. • The function of the ML feature (including the model inputs and outputs). • Instruction for installation, use, calibration, local validation and ongoing performance monitoring. • Compatible medical device, including software and hardware versions, and software and hardware requirement. • The clinical workflow of the device (including any human intervention). • Risks and limitations associated with the ML function. • Any exclusion criteria in the dataset used for training and validation
Description of the MLMD Model	• A description of the machine learning model (e.g. convolutional neural network) used in the MLMD, including any base model (e.g. Inception V3 model). • Demonstrate the appropriateness of the model for the MLMD's intended purpose. • Explain any limitations of the model, where applicable, mitigating measures to manage any shortcomings.
Model Inputs and Outputs	• A description of the input and output features. These can be in the form of diagnostic images, patient's historical records, physiological signals, medication records, handwritten text by healthcare professional, literature review, etc • Where pre-processing of data is required (e.g. signal pre-processing, image scaling), clearly defined the process and included in the submission. Provide a rationale for the pre-processing steps applied to the input data. • Built-in safeguard to ensure input meets the requirements.
Clinical Workflow during deployment	• Provide the intended or recommended workflow for deployment. • Identify the degree of human intervention in the clinical workflow. • The performance of the ML-human interaction for MLMD that involves human in the loop processes.
Model Training	• Provide the source and size of training dataset. • Clearly describe information on labelling of datasets, curation, annotation or other steps. • Provide a description on dataset cleaning and missing data imputation.

	• Developers must ensure that there is no duplication in training and validation datasets.
Performance Validation	• Based on the performance specification of the MLMD, provide test protocols and test reports. Provide metrics selected (e.g. classification accuracy, confusion matrix, logarithmic loss, area under curve (AUC)) to evaluate the performance of the machine learning model, along with the results of model evaluation. Refer to Section 3 of this document for the applicable information that should be provided. • Provide a breakdown of the test dataset and data collection protocol. This should address all potential biases and ensure that the test dataset is representative of the local population. • Provide information on control measures for detecting extremes/outliers. • Validate all performance claims (if any) with supporting evidence. • Clearly evaluate any limitations of the MLMD and communicated to the user in the product labelling or instruction manual.
Clinical Evaluation	
Clinical Association between the MLMD's output and clinical conditions(s) must be presented	• Present the presence of a valid clinical association between the MLMD's output and its targeted clinical condition. Refer to Section 3.5 for more information. • Clinical validation must ensure the software can be operated in clinical setting (e.g. operated by a specialist). The study design should include the rationale for the study population including (e.g. age, gender, sex, race, ethnicity, geographical location, medical condition) that represent the local population. The clinical validation data must be independent of the data used for training and tuning to demonstrate that the device is safe and effective for the intended population.
Risk Management	
Risk/Benefit Assessment	• Risk assessment should cover risks and vulnerabilities related to machine learning (e.g. overfitting, unintended bias, degradation, model drift) and risk controls implemented to eliminate or reduce these risks.

Table 1: Additional considerations for product registration for MLMD

9.2 Additional Considerations for MLMD with Continuous Learning Capabilities

MLMD with continuous learning capabilities can change their behaviour after deployment. The manufacturer must define the learning process and put appropriate process controls in place to effectively manage it. For example, implement appropriate quality checks to ensure that the quality of learning datasets is equivalent to that of the original training datasets. Incorporate validation processes within the system to closely

monitor the overall learning and the evolving performance of the MLMD post-learning. This monitoring is important to ensure that the learning does not compromise the defined specifications or output of the MLMD.

A MLMD with continuous learning capabilities can evolve and adapt following its market release. While this adaptability is advantageous, it also poses a risk: the system's performance may deteriorate over time without detection. Consequently, manufacturers must implement robust process controls to effectively manage these changes, thereby ensuring that the system remains both safe and effective as it continues to learn and evolve.

For continuous learning MLMD, submit complete information on the learning process including the process controls, verification, ongoing model monitoring measures for review in the MLMD registration application. Submit the following information (non-exhaustive) in addition to those requirements described in Table 7:

- A description of continuous learning process of the MLMD during deployment.
- Safety mechanism (built into the system) to detect anomalies and any inconsistencies in the output result and their mitigated strategies. These can include process to detect and roll-back to the previous algorithm version, including criteria which the system is measured against (baseline).
- During deployment, the MLMD will learn from real world data. Define the data source, data type collected, data pre-processing steps and parameter extracted to ensure there is no bias in the process. List the inclusion and exclusion criteria and ensure they are identical to the attributes of the original training dataset
- Process to ensure data integrity, reliability and validity of the new dataset used for learning.
- Implement software version controls, as the system has the potential for frequent updates and may possibility roll-back to the previous version at each deployment site.
- If the MLMD is deployed in a decentralised environment, robust processes should be implemented to address the risks involved in such a decentralised model.

Additional process controls to consider include maintaining traceability, performance monitoring and change management.

- Process to ensure traceability between real world data used for training, learning process, software version number and the MLMD's output during clinical use. When inaccurate results occur during deployment due to biased real world data, manufacturers must be able to trace back to the specific data, remove it from the AI model and retrain the models as necessary.
- Validation strategy and verification activities for continuous learning to ensure the performance remains within the pre-defined boundaries.

9.3 Post-market Monitoring of MLMD

Once MLMDs are deployed in the real-world environment, active monitoring, review and tuning are necessary[2]. Developers and distributors should establish process in collaboration with the implementers and users to ensure traceability. Implement mechanisms to monitor and review the performance of the MLMD deployed in clinical setting. Such monitoring may include autonomous monitoring embedded in the device. Implement a robust surveillance model to ensure that MLMD, especially those with continuous learning algorithms, maintain accuracy and prevent any concept drift. Developer should implement appropriate control measures based on post-deployment findings.

For all registered MLMD, companies must monitor the real-world performance post deployment. This allows close monitoring and detection of any failure, and where necessary, allows timely intervention post deployment of the MLMD. Refer to Section 6 for more information.

9.4 Changes to Registered MLMD

As with other registered medical devices, a Change Notification is required for any changes made to a registered MLMD. Please refer to the flowchart below and *GN-21: Guidance on Change Notification for Registered Medical Devices* to determine the category of change (e.g. Technical, Review or Notification) for changes to MLMDs.

[2] Model Artificial Intelligence Governance Framework Second Edition

(a) For all Medical Learning-enabled Medical Device MLMD (applicable for both locked and continuous learning algorithms)

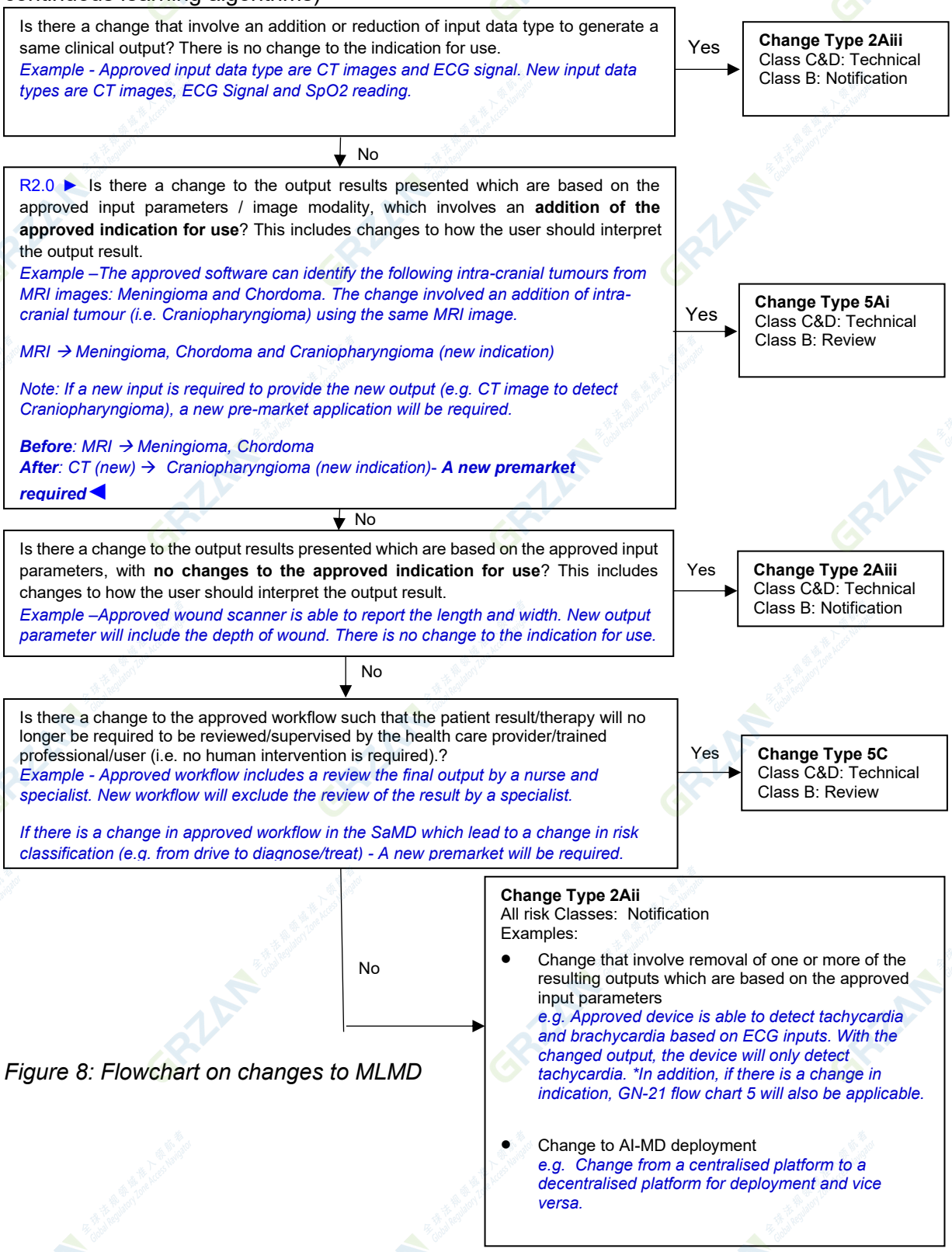


Figure 8: Flowchart on changes to MLMD

Note: With the change to MLMD, please note that GN-21 Flowcharts 2.3 and 2.4 remain applicable.

(b) For all Continuous Learning Algorithm **in addition to (a)**

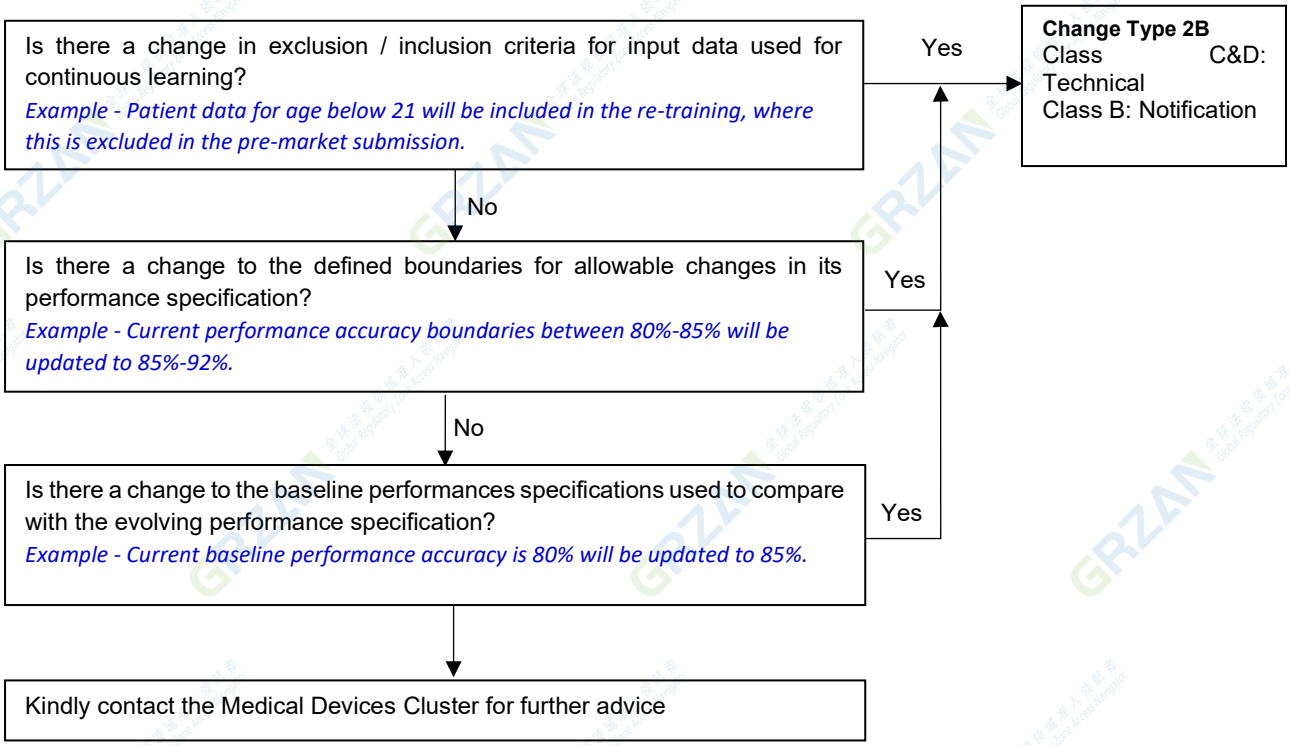


Figure 9: Flowchart for changes to MLMD incorporating continuous learning algorithm

Note: With the change to medical devices incorporating* continuous learning algorithm, *please note that GN-21 Flowcharts 2.3 and 2.4 and MLMD flowchart (a) remain applicable.

10. CHANGE MANAGEMENT PROGRAM (CMP)

Software as a Medical Device (SaMD) changes quickly and often. This creates challenges for manufacturers who need regulatory approval for software updates. This affects the timeline for implementing updates and gaining market access. To solve this problem, HSA created a new regulatory pathway called the Change Management Program (CMP) for SaMD. This includes SaMD with machine learning features. The CMP works with HSA's existing product registration and change notification processes. To enrol in CMP, companies must demonstrate their ability to maintain device safety and effectiveness through compliance with ISO 13485/MDSAP and IEC 62304 standards.

The CMP helps manufacturers implement software changes faster for SaMD registered on the Singapore Medical Device Register (SMDR). With CMP, manufacturers can implement pre-specified changes that would normally need a new Change Notification. After HSA approves these pre-specified changes, manufacturers can implement them using their Quality Management System. HSA will monitor these changes once the device is on the market. Companies must submit a declaration with their implementation record within one year of CMP approval, then submit annual declarations thereafter.

The CMP creates a flexible framework that supports fast changes in medical device technology, allowing timely software updates without compromising safety or performance.

For detailed information, please refer to *GN-37: Guidance on Change Management Program (CMP) for SaMD Including Machine Learning-Enabled SaMD.*

11. REFERENCES

i. IEC 62304 Medical device software – Software life cycle processes
ii. IEC/TR 80002-1:2009 Guidance on the application of ISO 14971 to medical device software
iii. ISO/IEC 22989:2022 Information Technology – Artificial Intelligence – Artificial Intelligence concepts and terminology
iv. ISO 13485:2016 Medical devices — Quality management systems — Requirements for regulatory purposes
v. ISO 14971: 2019 Medical devices — Application of risk management to medical devices
vi. ISO 81001-1:2021 Health software and health IT systems safety, effectiveness and security. Part 1: Principles and concepts
vii. ISO 81001-5-1: Health software and health IT systems safety, effectiveness and security. Part 5-1: Security — Activities in the product life cycle
viii. SS 620:2016 Good distribution practise for medical devices – Requirements
ix. Singapore Standards Council, TR 67:2018 Connected medical device security
x. IMDRF, Good machine learning practice for medical device development: Guiding Principles,
xi. IMDRF, Machine Learning-enabled Medical Devices: Key Terms and Definitions
xii. IMDRF, Software as a Medical Device (SaMD): Application of Quality Management System
xiii. IMDRF, Software as a Medical Device (SaMD): Clinical Evaluation
xiv. IMDRF, Software as a Medical Device (SaMD): Key Definitions
xv. IMDRF, Software as a Medical Device (SaMD): Possible Framework for Risk Categorization and Corresponding Considerations

HEALTH SCIENCES AUTHORITY

Health Products Regulation Group
Blood Services Group
Applied Sciences Group

www.hsa.gov.sg

Contact Information:

Medical Devices Cluster
Health Products Regulation Group
Health Sciences Authority

11 Biopolis Way, #11-03 Helios
Singapore 138667
www.hsa.gov.sg

HSA
Health Sciences Authority