HEALTH SCIENCES AUTHORITY

DECEMBER 2019

Regulatory Guidelines for Software Medical Devices – A Lifecycle Approach

HSA
Health Sciences Authority

Contents

1. INTRODUCTION

Software plays an increasingly important role in medical devices as a myriad of medical devices rely on software for safe and effective function, as well as for interoperability with other devices. In addition, emerging technologies like Artificial Intelligence and the Internet of Things (IOT) are being increasingly adopted for clinical applications, which introduces new and complex challenges (e.g. cybersecurity) to manufacturers who are developing medical device software.

To address this, all software medical device manufacturers are recommended to adopt a Total Product Life Cycle (TPLC) approach to manage and adapt to the rapid changes. This will include requirement management, risk assessment, software verification and validation, change management, traceability, and various aspects throughout a software's life cycle.

1.1. Objective

The Health Sciences Authority (HSA) is issuing these guidelines to provide clarity on the regulatory requirements for software medical devices in its entire life cycle. The requirements are presented starting from product development, all the way to post-market duties following product introduction in Singapore.

It is important to note that these guidelines reflect HSA’s current thinking and practice, and should not be misconstrued as a new regulatory control on software medical devices.

1.2. Intended Audience

The document is intended for stakeholders who are involved in software medical device development and /or supplying such devices in Singapore.

1.3. Scope

This document applies to software with intended use that falls under the definition of a medical device as stipulated in the *Health Products Act (HPA)*[1]. This includes software supplied in the following forms:

Forms of Software	Examples
Software embedded in medical devices	• Imaging software in diagnostic ultrasound system • Software to deliver pacing/defibrillation in a pacemaker/ ICD
Standalone software	• Image processing software (e.g. acquired from x-ray machine) that is intended to run on general purpose computer(s)
Standalone mobile applications	• Mobile application running on a mobile computing device that is intended to remotely monitor a patient’s vital signs For more examples, *please refer to Regulatory Guidelines for Telehealth Products. The guidelines can be found at* *https://www.hsa.gov.sg/medical-devices/guidance-documents*
Web-based software	• A software application that can be accessed through a web browser where users are able to upload patient images for diagnostic purpose without installation on their computing device

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

This document applies to software of all Risk Classifications and is intended to cover regulatory requirements spanning the entire product life cycle. Additionally, it addresses key software-related regulatory requirements such as cybersecurity and requirements for Artificial Intelligence (AI) medical devices. These guidelines will also be reviewed and updated from time-to-time with the emergence of new software-related technologies and evolving risks.

Overall, 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
- Artificial Intelligence

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.

AI-MEDICAL DEVICE (AI-MD): refers to artificial intelligence solutions which are intended to be used for investigation, detection, diagnosis, monitoring, treatment or management of any medical condition, disease, anatomy or physiological process.

CYBERSECURITY: preservation of confidentiality, integrity and availability of information in the Cyberspace.

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.

MOBILE APPLICATION: a software application that runs on smartphones and other mobile communication devices.

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 SOFTWARE: 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

The purpose of this section is to:

- Create a bridge for software manufacturers who may not be familiar with medical device Quality Management System (QMS) and how a QMS is applicable to software medical devices.
- Introduce good practices relating to QMS, so as to ensure safety, quality and effectiveness of software medical devices.

2.1. Quality Management System Principles

All manufacturers of medical devices, including software medical devices should have a Quality Management System in place to ensure manufacturing quality and consistency. For software medical devices, good software quality and engineering practices are used to control the quality of software products. The international standard: *ISO 13485 – Medical Devices – Quality Management Systems – Requirements for regulatory purposes*, specifies requirements for a QMS that can be adopted by an organization involved in one or more stages of the life cycle of a medical device.

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

- A **leadership and organisation** structure *(Figure 2)* that provides leadership which forms the basis of management support and governance.

- A set of **life cycle supported processes** *(Figure 3)* which includes product planning; risk management; documentation and record control; configuration management and control; measurement, analysis and improvement; and outsource management. These should be applied throughout the software medical device product realisation activities.

- **Product realisation activities** *(Figure 4)* 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

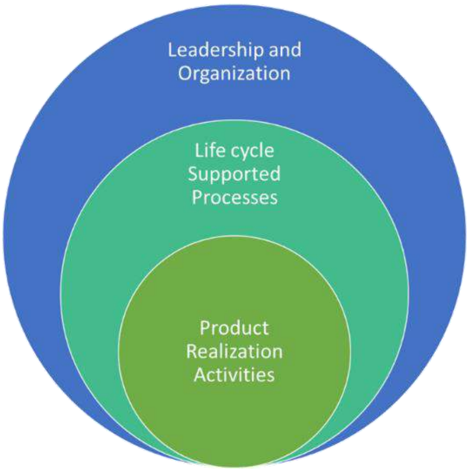

Leadership and Organization
Life cycle Supported Processes
Product Realization Activities

Figure 1: Quality Management Principles

The adoption of a QMS should be a strategic decision of an organisation. The design and implementation of an organisation's QMS is influenced by varying needs, its objectives, the products, the processes employed and the size and structure of the organisation.

2.1.1. Leadership and Organisation Support

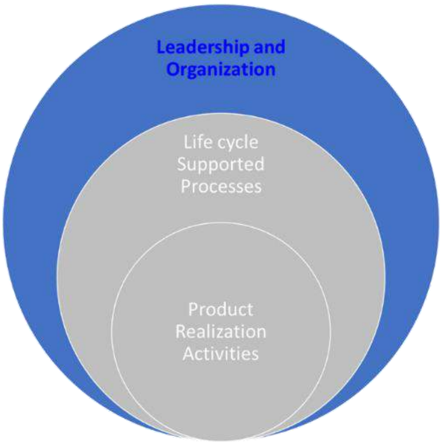

Leadership and Organization
Life cycle Supported Processes
Product Realization Activities

Figure 2: Leadership and Organisation Support

Management of the organisation forms the basis of the leadership and governance of all activities related to the life cycle processes including: defining the strategic direction, roles and responsibilities, authority, and communication to assure the safe and effective performance of the software medical device. In addition, top management shall ensure the availability and appropriate level of resources to ensure the effectiveness of the software medical device. The resources include: people, infrastructure, environment, tools etc. It is also important to ensure people who are assigned to the software medical device projects are competent and equipped with adequate skillsets, experience and training.

2.1.2. Life cycle Supported Processes

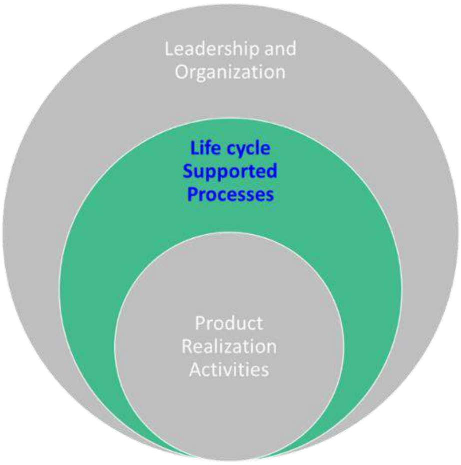

Leadership and Organization
Life cycle Supported Processes
Product Realization Activities

Figure 3: Life cycle Supported Processes

This refers to the important processes that support the software medical device life cycle:

- **Product Planning** – planning is not static; product plan needs to be updated when new information is gathered or a milestone is achieved.

- **Risk Management** – the risk management process should be integrated across the entire software medical device life cycle. Software risk management requires a balance of both safety as well as security features.

- **Document and Record Control** – no documentation is equal to no evidence. Records can be in paper or electronic form.

- **Configuration Management and Control** – source codes, releases, documents, software tools are important to maintain its integrity and traceability throughout the life cycle. It is also important to ensure the correct installation and integration of the software medical device into the clinical setting.

- **Measurement, Analysis and Improvement** – this includes the data obtained from post-market surveillances and monitoring, logging and tracking of complaints, problem reports, bug reports, non-conformity to product requirements. Data can be evaluated, analysed and feedback for improvement. Corrective actions are required when patient safety and device performance is compromised.

- **Outsource Management** – where any process, activities or products are outsourced, the organisation shall ensure control over such outsourced processes. When a commercial-off-the-shelf (COTS) software is chosen, used or integrated into the software medical device, the product owner of the software medical device is ultimately responsible for its safety and performance.

2.1.3. Product Realisation Activities

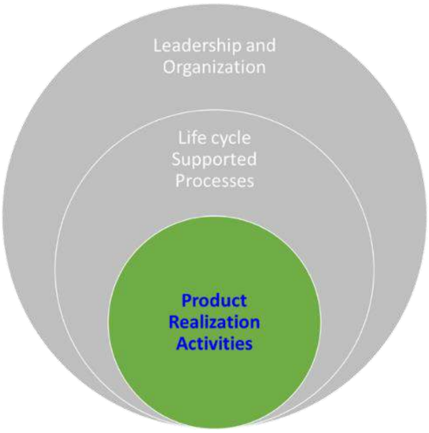

Leadership and Organization
Life cycle Supported Processes
Product Realization Activities

Figure 4: Product Realization

Product realisation forms the inner core activities of the QMS principles. It is supported by the outer cores: Leaderships & Organizations *(Figure 2)* and the Life Cycle Supported Processes *(Figure 3).*

An example of product realisation activities which are commonly found in software engineering life cycle approach are shown in *Figure 5* below. The product realisation activities mentioned here should be methodology (e.g. Waterfall, Agile, or V-model) agnostic.

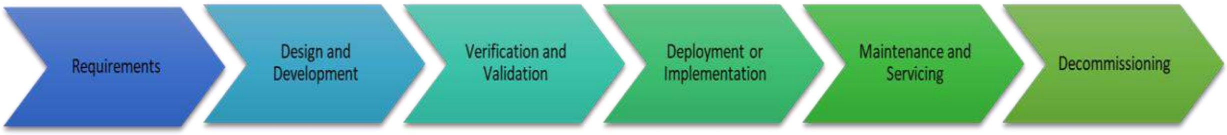

Requirements
Design and Development
Verification and Validation
Deployment or Implementation
Maintenance and Servicing
Decommissioning

Figure 5: Example of a typical software engineering life cycle approach for product realisation

- **Defining Requirements** – requirements captured must be in line with the intended use of the software medical device; and ensure user, patient and regulatory requirements are met.

Other aspects including: data integrity, usability engineering, interoperability and compatibility with different platforms or operating system and other medical devices subsystems should be considered during the requirements stage.

- **Design and Development** – activity to define the architecture, components and interfaces of the software system based on user requirements. Subsequently, it is translated into software items (codes, functions, libraries) and integrated into software medical device. Various clinical settings and home use environments where the software medical device is intended to be operated in, are to be considered during development. Risk mitigation, including security threats mitigation should be incorporated into the design as well.

- **Verification and Validation (V&V)** – Verification provides assurance that the design and development activities at each development stage conforms to the requirements, while Validation provides reasonable confidence that the software medical device meets its intended use or user needs. Information to be captured in the software verification and validation report includes: the tested software version number, the defined acceptance criteria, list of test cases, test results, any remaining anomalies, bugs or test deviations to be addressed and the overall validation conclusion.

- **Deployment or Implementation** – includes activities of: delivery, download, installation, setup and configurations to ensure the software can be delivered in a secure and reliable manner.

- **Maintenance and Servicing** – activities as a result of the following: changing of user requirements, through customer feedback or modification of previous deployed software medical device for preventive and corrective activities. Maintenance activities should preserve the integrity of the medical device software without introducing new safety, effectiveness, performance and security hazards. Risk assessment, hazard analysis and risk mitigation should be incorporated in every stages of the product realization to ensure all risks are addressed as early as possible in the life cycle.

- **Decommissioning** – activities to terminate maintenance, support and distribution of the software medical device, in a controlled ~~and managed~~ manner. Any patient data and other confidential data should be removed from the software or device to be decommissioned. This is important to minimize the impact to patients and public health safety as a result of the decommissioning medical device software during End-Of-Life (EOL).

3. PRE-MARKET PRODUCT REGISTRATION REQUIREMENTS

Product registration application for medical devices submitted to HSA must be prepared in the format set out in the ASEAN Common Submission Dossier Template (CSDT) document and may be prepared from the International Medical Device Regulators Forum (IMDRF) Non-In Vitro Diagnostic Medical Device Market Authorization Table of Contents (nIVD MA ToC). The mapping between the corresponding sections in the IMDRF ToC dossier and CSDT is available at https://www.hsa.gov.sg/medical-devices/guidance-documents

The various sections of the CSDT dossier and the respective contents are presented in our *GN17: Guidance on Preparation of a Product Registration Submission for General Medical Devices* using the ASEAN CSDT and *GN18: Guidance on Preparation of a Product Registration Submission for In Vitro Diagnostic (IVD) Medical Devices* using the ASEAN CSDT. The guidance can be found at https://www.hsa.gov.sg/medical-devices/guidance-documents

This section provides guidance for particular ~~certain~~ sections of the CSDT dossier where there may be specific requirements for software medical devices. Following are the sections covered here:

- Essential Principles for safety and performance of medical devices
- Labelling requirements
- Software versioning and traceability
- Software verification and validation
- Clinical evidence
- Risk management
- Supporting documents for cybersecurity

3.1. Essential Principles for Safety and Performance of Medical Devices

All medical devices, must be designed and manufactured to ensure that they are safe and perform as intended throughout the product life cycle. The Essential Principles for Safety and Performance checklist describes the fundamental design and manufacturing requirements. The design and manufacturing requirements that are relevant to a particular medical device must be identified and where requirements are deemed not applicable, the rationale has to be documented. This applies to all medical devices, including Class A medical device.

The developer of a medical device can refer to HSA's guidance document *GN-16: Guidance on Essential Principles for Safety and Performance of Medical Devices*. Essential Principles conformity checklists prepared using the "Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices" issued by the International Medical Device Regulators Forum (IMDRF) may also be submitted for device registration in Singapore.

The essential design and manufacturing principles that may be relevant to software medical devices are listed in Table 2 against the respective forms of software for reference.

Essential design and manufacturing principles	**Software embedded in medical devices**	**(i) Standalone software** **(ii) standalone mobile applications** **(iii) Web-based software**
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, implementation manual etc.) serves to help users: (i) identify the device; (ii) to communicate safety and performance related information; and (iii) ensure device traceability. Essential information such as name of device, software version number and product owner's information have to be presented on device labels for identification of the device. For safety and performance information, the intended purpose, instructions on proper use and safety information (e.g. contraindications) have to be clearly presented for users' reference.

Standalone software can be supplied in different forms and there may be difficulties in presenting device information for certain forms (e.g. web-based software). Generally, standalone software can be broadly categorised into two groups based on the mode of supply: i) supplied in physical form or ii) supplied without a physical form. The table below summarises the minimum labelling information to be included for standalone software supplied in either one of the two aforementioned ways.

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)	A screenshot of the splash screen which displays the elements for identification, including software version number. For downloadable software, if the downloading and installation is to be done by the end-user, the following information should be presented to the end-user: a) Internet address or web link to allow the end-user to download the software; b) The software download procedure; and c) The software installation guide or procedure.

	This ensures that the user has sufficient information for proper installation of such downloadable software. Although the software is supplied without physical form, the traceability of the software should not be compromised. An appropriate system for version controls and access rights controls should be in place 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 about labelling requirements for medical devices. The guidance can be found at https://www.hsa.gov.sg/medical-devices/guidance-documents

3.3. Software Versioning and Traceability

Software versioning is essential for identification and post-market traceability/follow-up in the event of software changes and field safety corrective actions. Description of software versioning and traceability system implemented for the software may be required during the registration process.

In addition, information on the software version being registered and to be supplied in Singapore is to be clearly presented. The software version information that represents all software changes/iteration (e.g. graphic interface, functionality, bug fixes) has to 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 ensure accuracy, reliability, precision, safety, and performance, while fulfilling their intended use.

The software verification process ensures that software specifications are met, by demonstrating that the design inputs generates the expected design outputs. The software validation process serves to ensure that the specifications capture the user's needs.

Software Verification & Validation report should include the results of all verification, validation and tests performed in-house and/or in a simulated user environment for the software prior to its final release. It should also provide objective evidence that demonstrates specified requirements are fulfilled and that defined software specifications conform to user needs and intended use. Reference to International Standards such as *IEC 62304: Medical device software – Software life cycle processes* is encouraged to demonstrate conformity to the essential requirements.

Any unresolved anomalies and deviations after the verification and validation testing must be appropriately reviewed and addressed. Assessment and justification for accepting these deviations and unresolved anomalies must be documented and provided during submission as well.

In cases where the software version number tested in the validation reports is different from the version for registration, a comparison of the two versions of the software together with the applicability and relevance of the report to the version for registration to be provided. The need for specific validation to address significant differences between the two versions has to be considered.

Medical devices are also becoming increasingly inter-connected. Hence, for medical devices that work together or in conjunction with other medical devices or systems, issues relating to the interoperability between such medical devices or systems have to be carefully considered and addressed as appropriate. Measures to ensure safe, secure and effective transfer and utilisation of information among these medical devices or systems have to be in place.

3.5. Clinical Evidence

While software verification and validation ensures that specified software system requirements and users' needs are met, clinical evaluation of software medical devices is conducted to support the safety and effectiveness of the software when used in the intended clinical environment.

The clinical evaluation process establishes that there is a valid clinical association between the software output and the specified clinical condition according to the product owner's intended use.

Clinical association refers to the extent to which the software's output (concept, conclusion, measurements) is clinically accepted or well-founded (existence of an established scientific framework or body of evidence) that corresponds accurately in the real world to the healthcare situation and condition referred in the software's defined intended purpose.

The association between the software output and clinical condition can be substantiated by one or more of the following:

- Referencing existing literature and well-established clinical guidelines;
- Comparison with similarly established software medical devices in the market and/or;
- Performing 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. Measures of clinical validation includes sensitivity, specificity, positive and negative predictive values etc.

Table 4 below summarises the type of clinical evidence recommended to support the clinical evaluation process for software medical devices. The level of clinical evidence required depends on the significance of the information generated by the software medical device (to treat or 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 ✓ Post-market Experience ✓ Clinical Studies	✓ Literature Reviews ✓ Post-market Experience	✓ Literature Reviews ✓ Post-market 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 ✓ Post-market Experience ✓ Clinical Studies	✓ Literature Reviews ✓ Post-market Experience	✓ Literature Reviews ✓ Post-market Experience
Non-Serious	✓ Literature Reviews	✓ Literature Reviews	✓ Literature Reviews

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.	✓ Post-market Experience ✓ Clinical Studies	✓ Post-market Experience	✓ Post-market Experience

Table 4: Clinical evidence requirements for software.

Where the software is assigned a novel intended purpose or is intended for use in new target populations, clinical studies should be carried out to support such use.

It is important to note that clinical evaluation should be an on-going process throughout the software life cycle. After the software medical device has been deployed in the market, clinical data should be collected to verify that the software continues to meet safety and effectiveness claims. Such continuous monitoring of the real-world clinical performance post-market allows for timely detection of new or evolving risks arising from the use of the software and to assess and update the risk-benefit assessment, where necessary. In addition, this may result in changes to the software (e.g. design change) or labelling (e.g. limitations of use) to enhance its safety and/or performance or to address risks or limitations in a timely manner.

3.6. Risk Management

Risk management should review and address all foreseeable risks and failure modes of the software in its product lifecycle. Risk assessment and evaluation should commensurate with the complexity and risk classification assigned to the software and also the defined intended purpose for the software. The principles described in "*ISO 14971 Medical Devices — Application of Risk Management to Medical Devices"* should be followed. In general, a systematic approach should be adopted in risk management: (i) identify all possible hazards, (ii) assess the associated risks, (iii) implement mitigations or controls to reduce risks to acceptable level and (iv) observe and evaluate effectiveness of mitigation measures.

For embedded software, the evaluation should also be based on the medical device system, which includes the hardware components.

Where there are changes made to a software, these should be systematically evaluated to determine if any additional risk could arise from these changes. Where necessary, additional risk control measures should be considered.

3.7. Cybersecurity

Minimum necessary requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to ensure the safe use of the software as intended should be implemented. For connected medical devices (e.g. with wireless features or internet-connected and network-connected functions), the following information should be submitted during registration:

i. Cybersecurity control measures in place (e.g. design controls)

ii. Cybersecurity vulnerabilities (known and foreseeable) and risk analysis and mitigation measures implemented;

iii. On-going plans, processes or mechanisms for surveillance, timely detection and management of the cybersecurity related threats during the useful life of the device, especially when a breach or vulnerability is detected in the post-market phase.

Please refer to *section 7* for details on overall cybersecurity management for software medical devices.

4. SOFTWARE MANUFACTURERS AND DISTRIBUTORS: ACTIVITY CONTROLS

All manufacturers, importers and/or wholesalers of software medical devices are required to hold medical device licences for the respective activities they perform. The pre-requisite for licencing is to implement and maintain an appropriate quality management system (QMS) which would cover the following aspects:

- Ensure the software is developed and manufactured under an appropriate and effective quality management system (e.g. ISO 13485 or GDPMDS)
- Ensure traceability of the software medical device. This is essential to track and trace the software (e.g. software version) to the users (e.g. physicians or patients) in the event of a Field Safety Corrective Action (FSCA) or product defect.
- Provide assurance that there is proper procedure in place for post-market surveillance and response. Ability to handle product recalls and implement corrective actions (e.g. bug fixes, cyber alerts, software patches) in a timely and effective manner (Planning, conducting and reporting of corrective action) and to identify any recurring problems requiring attention.
- Ensure proper maintenance and handling of device related records and information (e.g. customer complaints, distribution records, recall data) throughout the lifecycle of the software.

Refer to *GN-02: Guidance on Licensing for Manufacturers, Importers and Wholesalers of Medical Devices* for further information on the requirements. The guidance can be found at https://www.hsa.gov.sg/medical-devices/guidance-documents

There are certain circumstances unique to software medical devices and the below table presents our current position on the requirements related to QMS and licensing for these activities.

Do note that the software medical device will require product registration for all the scenarios mentioned below.

Possible scenarios	**Requirements for supply to Healthcare Institutions or other licensed distributors**
i. Local entities intending to import and distribute a software application in physical form (e.g. CD, USB and etc.)	• QMS based on ISO 13485 or GDPMDS • Importer's and Wholesaler's licences
ii. Local entities with authorisation from overseas developers/ product owners to provide access/distribute a software application through the internet or local	• QMS based on ISO 13485 or GDPMDS • Importer's and Wholesaler's licences

	online platforms (e.g. Apple App store, Google Play Store and etc.) where user will download and install the software application on their computing device	*Note: If the software application is supplied direct to general public, only Importer's licence is required*
iii.	Local entities intending to grant user access to a software application through a cloud service where hospital users are able to access it through the internet (usually web browser) without installation on their computing device	• QMS based on ISO 13485 or GDPMDS • Wholesaler's licence
iv.	Local entities intending to develop a software application locally. The software development will comprise of the designing, programming, testing and maintenance of the software application	• 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

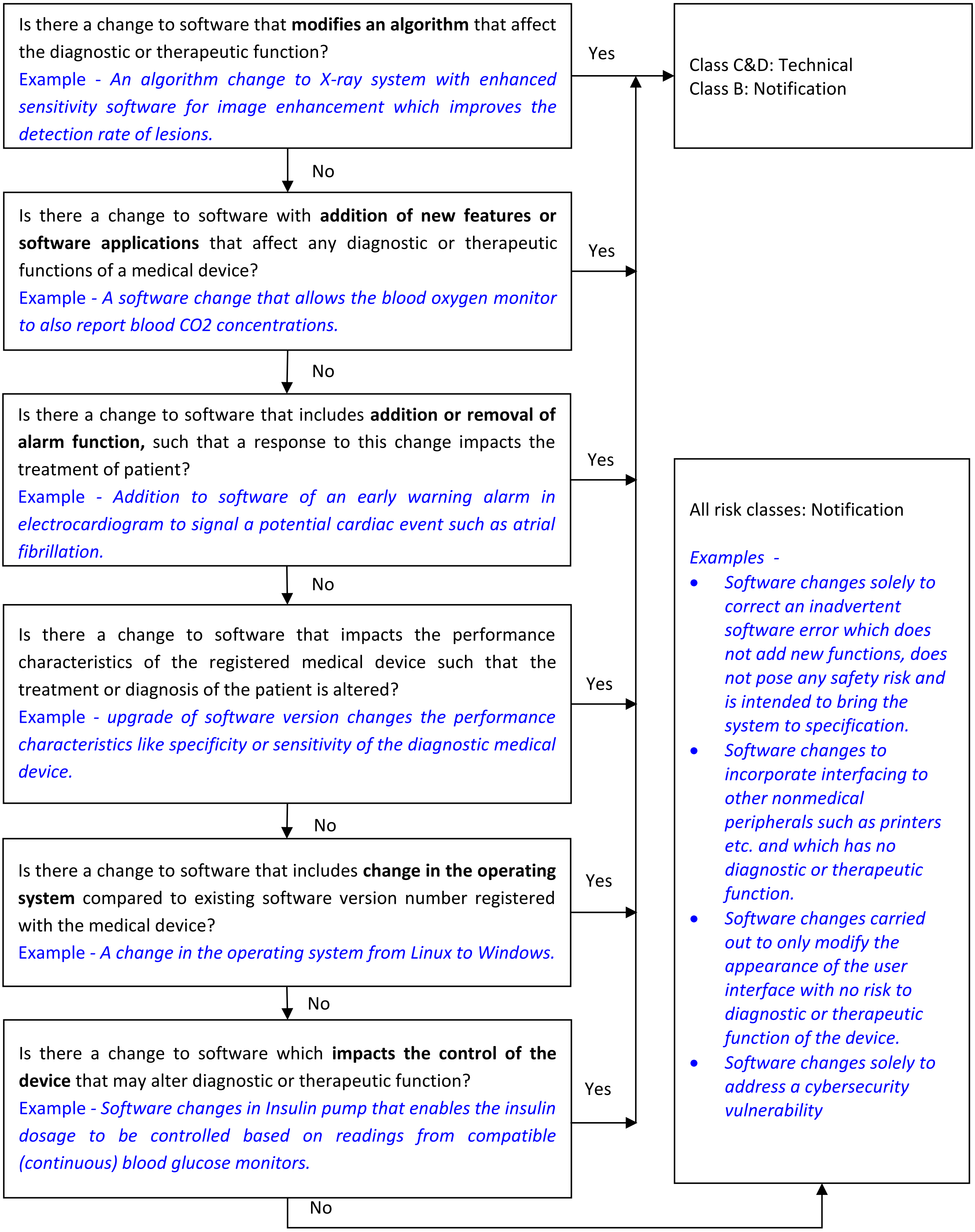
A software medical device undergoes a number of changes throughout its product life cycle. The changes are typically meant to (i) correct faults, (ii) improve the software functionality and performance to meet customer demands and (iii) ensure safety and effectiveness of the device is not compromised (e.g. security patch).

To address the range of changes with differing risk and complexity, HSA employs a risk-based approach to managing the changes to registered software; the regulatory requirements of the change shall commensurate with the significance of the change. For instance, significant changes (i.e. Technical & Review changes) will undergo a more in-depth review (when compared to a non-significant change) to ensure that the change does not affect the safety and effectiveness of the software.

As such, non-significant software changes are required to be notified to HSA and are referred to as Notification changes as described in the flowcharts below. Such Notification changes may be bundled together in one application (within a maximum of 6 months from the initiation of the change) or submitted together with other upcoming Review/Technical changes for the registered software. Do note that such bundled Notification changes are not allowed for AE/FSCA related changes and for changes to AI medical devices.

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

Changes to Software* of General Medical Devices (GMD)



Is there a change to software that **modifies an algorithm** that affect the diagnostic or therapeutic function?

Example - *An algorithm change to X-ray system with enhanced sensitivity software for image enhancement which improves the detection rate of lesions.*

Is there a change to software with **addition of new features or software applications** that affect any diagnostic or therapeutic functions of a medical device?

Example - *A software change that allows the blood oxygen monitor to also report blood CO2 concentrations.*

Is there a change to software that includes **addition or removal of alarm function,** such that a response to this change impacts the treatment of patient?

Example - *Addition to software of an early warning alarm in electrocardiogram to signal a potential cardiac event such as atrial fibrillation.*

Is there a change to software that impacts the performance characteristics of the registered medical device such that the treatment or diagnosis of the patient is altered?

Example - *upgrade of software version changes the performance characteristics like specificity or sensitivity of the diagnostic medical device.*

Is there a change to software that includes **change in the operating system** compared to existing software version number registered with the medical device?

Example - *A change in the operating system from Linux to Windows.*

Is there a change to software which **impacts the control of the device** that may alter diagnostic or therapeutic function?

Example - *Software changes in Insulin pump that enables the insulin dosage to be controlled based on readings from compatible (continuous) blood glucose monitors.*

Class C&D: Technical
Class B: Notification

All risk classes: Notification

Examples -

- *Software changes solely to correct an inadvertent software error which does not add new functions, does not pose any safety risk and is intended to bring the system to specification.*
- *Software changes to incorporate interfacing to other nonmedical peripherals such as printers etc. and which has no diagnostic or therapeutic function.*
- *Software changes carried out to only modify the appearance of the user interface with no risk to diagnostic or therapeutic function of the device.*
- *Software changes solely to address a cybersecurity vulnerability*

Figure 6: Flowchart for the changes to software of a GMD.

**Software refers to Standalone software/mobile applications and/or Software embedded in medical device system.*

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

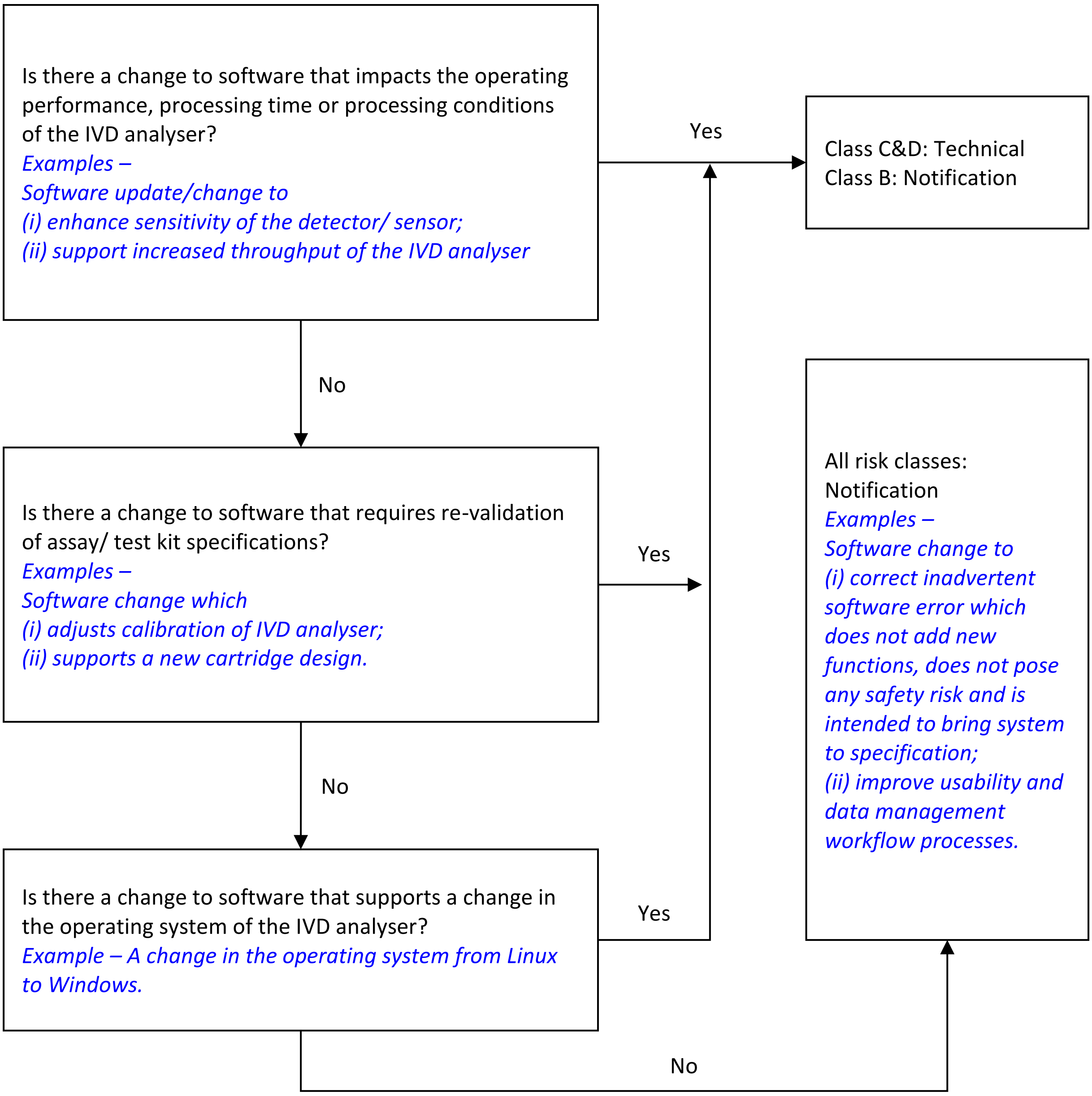

Is there a change to software that impacts the operating performance, processing time or processing conditions of the IVD analyser?
Examples –
Software update/change to
(i) enhance sensitivity of the detector/ sensor;
(ii) support increased throughput of the IVD analyser
Yes
Class C&D: Technical
Class B: Notification
No
Is there a change to software that requires re-validation of assay/ test kit specifications?
Examples –
Software change which
(i) adjusts calibration of IVD analyser;
(ii) supports a new cartridge design.
Yes
No
All risk classes: Notification
Examples –
Software change to
(i) correct inadvertent software error which does not add new functions, does not pose any safety risk and is intended to bring system to specification;
(ii) improve usability and data management workflow processes.
Is there a change to software that supports a change in the operating system of the IVD analyser?
Example – A change in the operating system from Linux to Windows.
Yes
No

Figure 7: Flowchart for the changes to software of an IVD medical device.

Please note that changes made to software medical devices are not only limited to the above two flow charts. Other flowcharts in GN-21 will still be applicable depending on the actual change types (e.g. expansion of indications of use of the software). All principles described in GN-21 will apply, to software medical devices.

6. POST-MARKET MANAGEMENT OF SOFTWARE MEDICAL DEVICES

Post-market monitoring and surveillance of software medical devices allows timely identification of software-related problems, which may not be observed during device development, validation and clinical evaluation since these are performed in controlled settings. New risks may surface when the software is implemented in a broader real world context and is used by diverse spectrum of users with different expertise.

Companies involved in distributing software medical devices in Singapore (manufacturers, importers, wholesalers and registrants) are required to comply with their post-market duties and obligations which includes reporting of device defects or malfunctions, recalls, Field Safety Corrective Actions and serious injuries or death associated with use of the device.

This section presents an overview of some of these post-market requirements that are also applicable to software medical devices.

6.1. Field Safety Corrective Actions (FSCA)

With the increasing usage of software in medical systems coupled with the complexity of such devices, it is expected that the number of software issues affecting such medical devices will also increase. These software medical systems are often critical systems, which the healthcare providers and/or patients rely on therefore, the proper functioning of these systems is essential.

Understanding the cause of the software issue not only ensures safety of patients, but also provides manufacturers an opportunity to improve safety and performance of these devices by learning from actual use and incorporating such information into the product design and development. .

A FSCA may be initiated when the product owner becomes aware of certain risks associated with use of the medical device through post-market monitoring and surveillance, such as through tracking of product complaints / feedback. The product owner typically initiates a FSCA to communicate the risks to users and inform of the measures to be implemented to mitigate the risks.

For software medical devices, issues commonly encountered include (non-exhaustive list) the following:

- 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
- Potential clinical 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 display of images e.g. flipped images when exported; display errors such as screen blank-outs or frozen screens
- Errors in calculation 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 errors e.g. Graphical User Interface (GUI) related issues

Software errors or bugs may be introduced during design and development of the device and also during use of the device. The following lists some possible causes of software errors:

- Input of incorrect, incomplete or inconsistent requirements and specifications
- Incomplete or lack of validation of software prior to initial release
- Failure to examine the impact of changes during software upgrades or bug fixes
- Incorrect configuration e.g. failure to upgrade accompanying operating system
- Incompatibility with 3rd party installed program
- Software does not properly interface with external devices or other software components/modules

Some not so obvious cause for software-related errors include lack of or improper documentation of procedures e.g. inadequate instructions on use, improper installation guidelines, etc.

Corrective and preventive actions to address such issues typically includes implementation of bug fixes or updates to the existing software. At times, the issue may not be caused by the software (e.g. battery circuit fault resulting in reduced battery life), however, a software upgrade may serve as one of the corrective actions to mitigate the risk (e.g. introduction of alarm function to notify users to change the battery when a specified number of cycles has been met).

For correction of devices affected by FSCA, correction should proceed without undue delay upon availability of the software upgrade or bug fix. Service reports for completion of the software upgrade should clearly document the software version installed and kept on file for traceability purposes.

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

6.2. Adverse Events

As part of the post-market duties and obligations, companies involved in distributing medical devices in Singapore (manufacturers, importers, wholesalers and registrants) are required to report Adverse Events (AE) associated with the use of software medical devices. The objective of AE reporting and investigation is to reduce the likelihood of, or prevent recurrence of the AE and/or to alleviate consequences of such recurrence.

Adverse events involving software medical devices may directly or indirectly, have an impact on patients and users. For example, failure of software-controlled devices such as insulin pumps, which senses blood sugar levels periodically and injects insulin to maintain normal levels of blood sugar, may result in hypoglycaemia that can be life-threatening when left undetected. Indirect harm to patients may occur in AEs involving devices such as IVD analysers that include software that control and manage their performance. Software errors may lead to incorrect or inaccurate patient results and consequently, result in wrong diagnosis and potentially incorrect treatment for the patient.

Reports may come from various sources including surveillance of device log sheets, complaints or feedback from the user. Prompt investigation on the reports and timely implementation of corrective and/or preventive actions are necessary to manage the risks and ensure that the AE does not recur.

AEs for software medical devices may arise due to (non-exhaustive list):

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

7. CYBERSECURITY

7.1. Importance of Cybersecurity

Cybersecurity is critical in today's interconnected world, with medical devices becoming more connected (e.g. wireless, Internet, or network-connected). Cybersecurity attacks can fatally disrupt medical devices availability and/or functionality, and may render hospital networks unavailable, delaying patient care. Only with competent cybersecurity, medical devices functionality and safety can be effectively protected. For software medical devices that has the capability to communicate/connect with other systems, it is crucial for manufacturers to consider an effective cybersecurity strategy that addresses all possible cybersecurity risks not only during development but throughout the useful life of the software medical device.

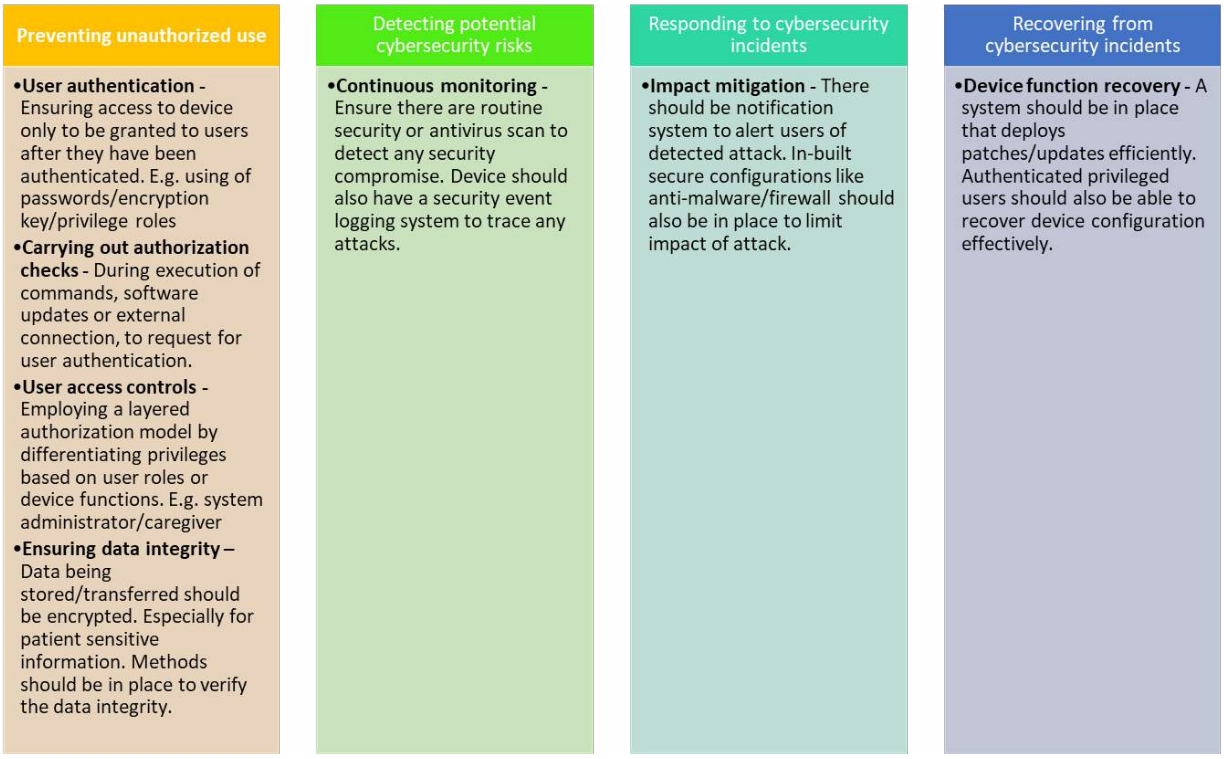
Cybersecurity especially for medical devices cannot be achieved by a single stakeholder, it requires the concerted effort of diverse stakeholders (government agencies, manufacturers, healthcare institutions, users of medical devices). Continuous monitoring, assessing, mitigating and communicating cybersecurity risks and attacks requires active participation by all stakeholders in the ecosystem.

7.2. Cybersecurity Considerations

When developing a software medical device, a cybersecurity plan should be devised to include the following considerations, (non-exhaustive): (i) a secure device design, (ii) having proper customer security documentation, (iii) conduct cyber risk management, (iv) conduct verification and validation testing and, (v) having an on-going plan for surveillance and timely detection of emerging threats

7.2.1. Secure Device Design

Cybersecurity should be considered from the early stages of device design and development. Manufacturers should take into account all possible cybersecurity hazards and consider design inputs that could reasonably secure the device and prevent, detect, respond and where possible recover from foreseeable cyber risks. Below are some possible design considerations.



Preventing unauthorized use	Detecting potential cybersecurity risks	Responding to cybersecurity incidents	Recovering from cybersecurity incidents
•**User authentication -** Ensuring access to device only to be granted to users after they have been authenticated. E.g. using of passwords/encryption key/privilege roles •**Carrying out authorization checks -** During execution of commands, software updates or external connection, to request for user authentication. •**User access controls -** Employing a layered authorization model by differentiating privileges based on user roles or device functions. E.g. system administrator/caregiver •**Ensuring data integrity –** Data being stored/transferred should be encrypted. Especially for patient sensitive information. Methods should be in place to verify the data integrity.	•**Continuous monitoring -** Ensure there are routine security or antivirus scan to detect any security compromise. Device should also have a security event logging system to trace any attacks.	•**Impact mitigation -** There should be notification system to alert users of detected attack. In-built secure configurations like anti-malware/firewall should also be in place to limit impact of attack.	•**Device function recovery -** A system should be in place that deploys patches/updates efficiently. Authenticated privileged users should also be able to recover device configuration effectively.

Figure 7: Cybersecurity design considerations (non-exhaustive)

7.2.2. Customer Security Documentation

Besides supplying the end users with the Instructions for use (IFU) on the appropriate usage of the medical device, manufacturers should also consider providing a customer security documentation to communicate the relevant security information to mitigate cybersecurity risks when operating the medical device in its intended use environment. The following information should be considered in the Customer Security Documentation (by the manufacturer):

- End users should be informed on the possible cybersecurity hazards that the software medical device poses. There should also be advice given on how and what they can do to mitigate the risk of those cybersecurity hazards (e.g. connecting only to protected network, anti-virus, firewall). This information to the end users could also be presented in the instruction manual or label of the device.

- Recommended infrastructure requirements to support the device in its intended use environment.

- A list of network ports and other interfaces that are expected to receive and/or send data, and a description of port functionality and whether the ports are incoming or outgoing. This may allow users to consider disabling unused ports to prevent unauthorised access to the device.

- The procedures to download and install updates from the manufacturer.

- Information, if known, concerning device cybersecurity end of support. This will allow the users to understand their responsibilities and device risks after the device has exceeded its end of support period.

- A Software Bill of Material (SBOM) including but not limited to a list of commercial, open source, and off-the-shelf software components including the version and build of the components, to enable device users (including patients and healthcare providers) to effectively manage their assets, to understand the potential impact of identified vulnerabilities to the device (and the connected system) and to deploy countermeasures to maintain the device's safety and performance.

7.2.3. Cyber Risk Management

When managing cybersecurity risks, the principles described in ISO 14971 should also be followed. There may be some device specific cybersecurity risk involved but generally, manufacturers should include the following in their risk management plan: (i) identify all possible cybersecurity hazards, (ii) assess the associated risks, (iii) implement mitigations or controls to reduce risks to acceptable level and, (iv) observe and evaluate effectiveness of mitigation measures.

The risk management process should be carried out consistently throughout the software life cycle and there should be proper documentation (e.g. a report). Some critical components that should be incorporated into the risk management plan are as follows:

- Employing tools such as threat modelling to identify vulnerabilities and develop mitigation after risk evaluation.

- Cybersecurity risk management process should be conducted in parallel with safety risk management. The overall patient safety should be considered when introducing security measures prevent any unintentional patient harm. For instance, implementing multi-factor authentication before accessing a CT device, might cause the device to not be readily accessible during emergency, as such, an emergency mode may be considered to address the safety risk.

- Establishing an on-going program for monitoring and surveillance of threats and vulnerabilities. If new cybersecurity vulnerabilities are discovered, manufacturers are strongly recommended to conduct vulnerability risk assessment to evaluate the potential for patient harm and compromise of device performance. The vulnerability can be analysed by taking into consideration (i) the exploitability of the vulnerability, and (ii) the severity of user/patient harm if the vulnerability were to be exploited. This assessment can allow determination of whether the risk involved is controlled or uncontrolled. If it is deemed that mitigating measures or compensating controls are required to mitigate the risk, manufacturer should practise vulnerability disclosure to communicate to all affected users & stakeholders effectively. Such information could include identification of affected devices, vulnerability impact, mitigations/ compensating controls etc.).

- Monitoring all software (including 3rd party software) for new vulnerabilities and risks which may affect the safety and performance of the device.

- Implementing a process for timely detection and analysis of vulnerabilities and threats, including impact assessment and follow-up actions to take e.g. containment of threats, communication to affected parties, fixing of vulnerabilities.

7.2.4. Verification and Validation

Implemented cybersecurity risk control methods should be verified and validated against specified design requirements or specifications prior to implementation. The features and functions should remain operative for device to carry out its intended use even with the presence of those residual cybersecurity risks. Some possible cybersecurity tests include malware test, structured penetration test, vulnerability scanning etc.

7.2.5. On-going plan for surveillance and timely detection of emerging threats

As medical device systems are becoming more complex, the nature of cybersecurity threats has also evolved rapidly. Healthcare systems are especially vulnerable, given the number of medical devices that are connected to the hospital networks.

It is therefore, not possible to rely solely on premarket controls to mitigate all cybersecurity risks. Manufacturers of software medical devices should establish a comprehensive and structured cybersecurity risk management plan for the entire software life cycle.

Manufacturers should have an initiative to actively survey and detect possible threats as part of their post-market plan. There should be a plan outlined by the manufacturers on how they can actively monitor and respond to evolving and newly identified threats. Key considerations for this post-market plan include:

Post-market Vigilance	A plan to proactively monitor and identify newly discovered cybersecurity vulnerabilities, assess their threat, and respond
Vulnerability Disclosure	A formalized process for gathering information from vulnerability finders, developing mitigation and remediation strategies, and disclosing the existence of vulnerabilities and mitigation or remediation approaches to stakeholders.
Patching and Updates	A plan outlining how software will be updated to maintain ongoing safety and performance of the device either regularly or in response to an identified vulnerability
Recovery	A recovery plan for either the manufacturer, user, or both to restore the device to its normal operating condition following a cybersecurity incident.
Information sharing	Involve in the communication and sharing of updated information about security threats and vulnerabilities. For example, participation in Information Sharing Organizations (e.g. ISAOs, ISACs and etc.).

Table 6: Cybersecurity post-market planning

7.3. Patient Confidentiality and Privacy and Other Regulations

Medical device cybersecurity incidents can affect patient safety and privacy. There are increasing reports of breaches of data privacy. Software medical device developers, implementers and users should always be vigilant in handling confidential patient data. Local legislation and regulations on data protection and privacy should be complied with (e.g. Infocomm Media Development Authority (IMDA)'s Personal Data Protection Act (PDPA)). Please take note that it is the responsibility of the manufacturers and distributors to ensure that the medical device meets the requirements of any other applicable regulatory controls in Singapore.

8. ARTIFICIAL INTELLIGENCE MEDICAL DEVICES (AI-MD)

This section presents some additional regulatory considerations specific to medical devices incorporating Artificial Intelligence (AI) from a medical device regulatory standpoint.

Developers and implementers of AI-MDs are to ensure that there are measures in place to ensure the responsible development and deployment of AI-MD. Other relevant legislation and guidelines applicable to the development and deployment of AI-MD in healthcare should be complied with. For e.g.:

- Personal Data Protection Act
- Human Biomedical Research Act
- Private Hospitals and Medical Clinics Act

8.1. Regulatory Requirements for AI-MD

The regulatory principles for AI-MDs are comparable to software that are regulated as medical devices However, there are specific additional considerations such as continuous learning capabilities, level of human intervention, training of models, retraining etc. for AI-MD that need to be considered carefully and addressed.

All activities related to the design, development, training, validation, retraining and deployment of AI-MD should be performed and managed under an ISO 13485 based quality management system (QMS). Please refer section 2 in this document for further information.

The block diagram below illustrates the process of developing and deployment of the AI-MD.

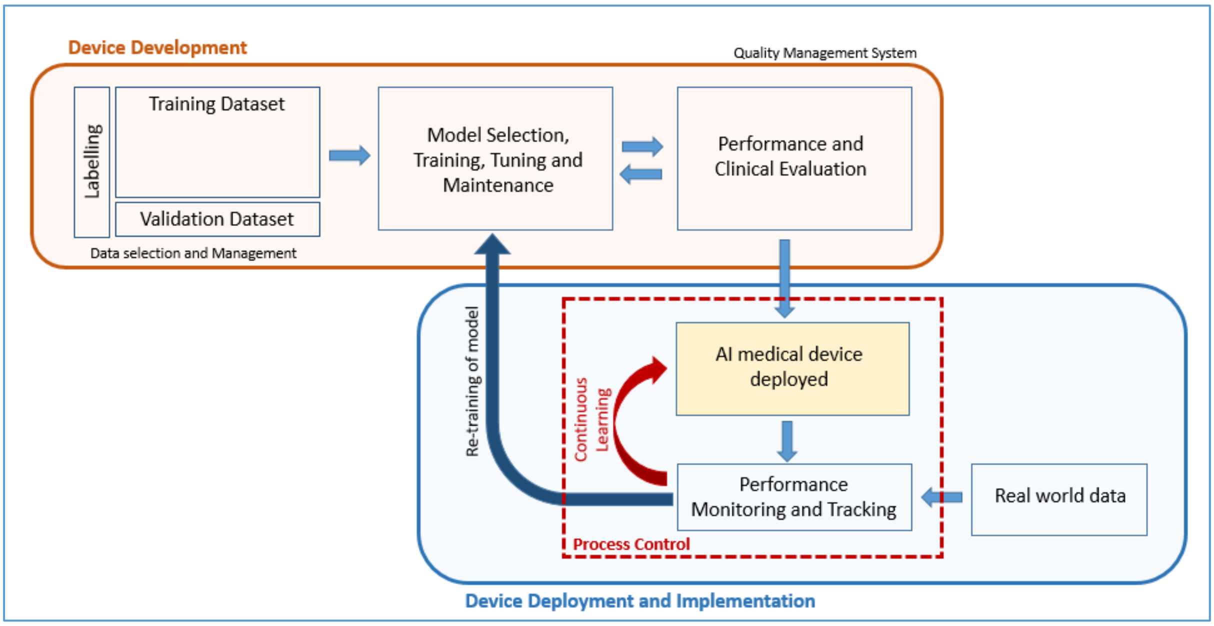

Device Development
Quality Management System
Labelling
Training Dataset
Validation Dataset
Data selection and Management
Model Selection, Training, Tuning and Maintenance
Performance and Clinical Evaluation
Re-training of model
Continuous Learning
AI medical device deployed
Performance Monitoring and Tracking
Real world data
Process Control
Device Deployment and Implementation

Figure 8: Typical illustration of an AI model

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

Requirements	Description
Dataset	

Input data and features/ attributes used to generate the corresponding output	This should include the various input data and features/ attributes selected for the AI-MD to generate the corresponding output result. This can be in the form of diagnostic images, patient's historical records, physiological signals, medication records, handwritten text by healthcare professional, literature review, etc. The specifications or acceptance criteria for selecting the input data and features/ attributes has to be defined. In the event where pre-processing (e.g. signal pre-processing, image scaling,) of data is required, the process should be clearly defined and included in the submission. Rationale has to be provided for the pre-processing steps applied to the input data.
Source, size and attribution of training, validation and test datasets	The source and size of training, validation and test dataset should be provided. Information on labelling of datasets, curation, annotation or other steps should be clearly presented. Description on dataset cleaning and missing data imputation should be provided. Developer should also ensure that there is no duplication in training and validation datasets. Rationale for the appropriateness and adequacy of the dataset selected and possible factors that can potentially influence the output result must be provided. In addition, all potential biasness in selecting the training and validation dataset should be adequately addressed and managed.
AI Model	
AI model selection	A description on the machine learning model (e.g. convolutional neural network) used in the AI-MD, including any base model (e.g. Inception V3 model), should be provided. Appropriateness of the model for the AI-MD's intended purpose should be presented. Any limitations of the model and where applicable mitigating measures to manage any shortcomings should also be explained. Model evaluation should be performed using a test dataset that is separate from the training dataset. Metrics (e.g. classification accuracy, confusion matrix, logarithmic loss, area under curve (AUC)) selected to evaluate the performance of the machine learning model selected should be provided, including the results of model evaluation.
Performance and Clinical Evaluation	
Test protocol and report for verification and validation of the AI-MD, including the acceptance limits and information on the anomalies identified	Based on the performance specification of the AI-MD, the test protocol and test report should be provided. Please refer to section 3 of this document and where applicable this information should be provided. Information on control measures to detect extremes/outliers should be provided.

	Any limitation of the AI-MD and the operating system must be clearly evaluated and also communicated as appropriate to the user in the product labelling or instruction manual.
Performance of the AI-MD (e.g. diagnostic sensitivity/specificity /reproducibility where applicable	The performance specification such as accuracy, specificity and sensitivity of the device should be provided (e.g. Accuracy 90%, Sensitivity 91-93%, Specificity 95%). Validation and verification test report(s) has to be provided to substantiate such performance claim.
Clinical Association between the AI-MD's output and clinical conditions(s) must be presented	Presence of a valid clinical association between the AI-MD's output and its targeted clinical condition should be demonstrated by appropriately designed clinical studies.
Deployment	
Device workflow including how the output result should be used	The intended or recommended workflow during the deployment of the device should be presented and explained. When there is human intervention in the system (human-in-the-loop), the workflow should clearly indicate the degree of intervention and the stage(s) in the workflow for the intervention.
Interval for training data update cycle (e.g. in months or years)	In cases where data is collected after the deployment of the AI-MD (fixed-version) and these datasets are used to re-train the subsequent models of the AI-MD, information on the interval for training data update cycle has to be provided. If a new set of data collected changes the original specification and performance of the device, a Change Notification should be submitted to HSA. Similar to other software, a Change Notification will be required for changes to registered AI-MDs. This includes any changes to the performance specifications, input data types, device workflow, degree of human intervention, choice of AI model, etc. Decision flow presented in section 5 of this document is also applicable to AI-MDs
Software version to be supplied in Singapore and the procedure or plan implemented to trace the software version for subsequent iterations	For the purpose of post-market traceability, the exact AI-MD version to be supplied in Singapore and explanation on how the version numbers are designated and traced should be provided.

Table 7: Additional considerations for product registration for AI-MD

8.2. Additional Considerations for AI-MD with Continuous Learning Capabilities

AI-MD with continuous learning capabilities has the ability to change its behaviour post deployment. The learning process should be defined by the manufacturer and appropriate process controls should be put in place to effectively control and manage the learning process. For example, there should be appropriate quality checks to ensure that the quality of learning datasets are equivalent to the quality of the original training datasets. There should be validation processes incorporated within the system to closely monitor the overall learning and the evolving performance of the AI-MD post-learning. This is important to ensure that the learning does not compromise the defined specifications or output of the AI-MD. As the AI-MD with continuous learning capabilities can automatically change its behaviour post deployment, it is essential for the manufacturer to ensure there is a robust process control in place. This can ensure that the performance of the AI-MD does not deteriorate over time.

For continuous learning AI-MDs, complete information on the learning process including the process controls, verification, ongoing model monitoring measures shall be clearly presented for review in the application for registration of the AI-MD. The following information (non-exhaustive) in addition to those requirements described in Table 7 should be submitted.

- Description on the process of continuous learning of the AI-MD during deployment.

- Safety mechanism (can be built into the system) to detect anomalies and any inconsistencies in the output result and how these are mitigated. This can include process to detect and roll-back to the previous algorithm version which includes criteria by which the system is measured against (baseline).

- During deployment, the AI-MD will learn from real world data. The source, datatype collected, data pre-processing steps and parameter extracted should be defined to ensure there are no biasness in the process. The inclusion and exclusion criteria should be listed and this should be identical to the attributes of the original training dataset

- Process to ensure data integrity, reliability and validity of the new data set used for learning

- Software version controls should be in place as the system has the potential for frequent updates and possibility for roll-back to the previous version in each of the deployment site.

  If the AI-MD is deployed in a decentralised environment, there should be robust processes in place to address the risks involved in such a decentralised model. Other process controls for consideration includes maintaining traceability, performance monitoring and change management.

- Process to ensure traceability between real world data for training, learning process, system version number and the AI-MD's output during clinical use. When there are inaccurate results during deployment due to bias real world data, manufacturer must be able to trace back to the specific data and remove such data from the AI model and retrain the models as necessary.

- Validation strategy and verification activities for continuous learning to ensure the performance is within the pre-defined boundaries / envelope

8.3. Post-market Monitoring of AI-MD

Once AI-MDs are deployed in the real-world environment, active monitoring, review and tuning are necessary[2]. Developers and distributors should establish a process in collaboration with the implementers and users to ensure traceability and also implement mechanisms to monitor and review the performance of the AI-MD deployed in clinical setting. Such monitoring could also be in the form

[2] Model Artificial Intelligence Governance Framework First Edition

of autonomous monitoring embedded in the system. A robust surveillance model to ensure that the AI-MD especially those with continuous learning algorithms remain accurate and to prevent any concept drift should be implemented.

For all registered AI-MDs locally, companies are required to monitor the real-world performance post deployment and submit periodic post-market reports to HSA. This allows close monitoring and detection of any failure of these AI-MDs by HSA and where necessary enables timely intervention post deployment of the AI-MD.

8.4 **CHANGES TO A REGISTERED AI-MD**

Similar to other registered medical devices, a Change Notification will be required for any changes made to a registered AI-MD. The following are some of the changes made to an AI-MD which will require a submission of Change Notification (non-exhaustive):

- Change in AI algorithm or model that affect the diagnostic or therapeutic function
- Change that involves addition or reduction of input data type or the features extracted from the input data
- Change that involves addition of the output results presented to the user. This includes changes to how user should interpret the output result
- Change in the performance specifications of the device
- Removal of human intervention approved in the intended workflow
- Change from a centralised platform to a decentralised platform for deployment and vice versa

Additional changes for AI-MD with continuous learning algorithm (non-exhaustive):

- Change in exclusion / inclusion criteria for input data used for continuous learning algorithm
- Change to the defined boundaries / envelop for allowable changes in its performance specification
- Change to the baseline performance specifications used to compare with the evolving performance specification

Please refer to section 5 of this document for more information.

9. REFERENCES

i. IEC 62304 Medical device software – Software life cycle processes

ii. IMDRF. Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices, 31 October 2018

iii. IMDRF, Software as a Medical Device (SaMD): Clinical Evaluation, 21 September 2017

iv. IMDRF, Software as a Medical Device (SaMD): Application of Quality Management System, 2 October 2015

v. IMDRF, Software as a Medical Device (SaMD): Possible Framework for Risk Categorization and Corresponding Considerations, 18 September 2014

vi. IMDRF, Software as a Medical Device (SaMD): Key Definitions, 18 December 2013

vii. Singapore Standards Council, TR 67:2018 Connected medical device security, 2018

viii. ISO 13485:2003 Medical devices — Quality management systems — Requirements for regulatory purposes

ix. ISO 13485:2016 Medical devices — Quality management systems — Requirements for regulatory purposes

x. SS 620:2016 Good distribution practise for medical devices – Requirements

xi. ISO 14971:2007 Medical devices — Application of risk management to medical devices

xii. IEC/TR 80002-1:2009 Guidance on the application of ISO 14971 to medical device software

HEALTH SCIENCES AUTHORITY

Health Products Regulation Group
Blood Services Group
Applied Sciences Group

www.hsa.gov.sg

Contact Information:

Medical Devices Branch
Medical Devices Cluster
Health Products Regulation Group
Health Sciences Authority

11 Biopolis Way, #11-03 Helios
Singapore 138667
www.hsa.gov.sg
https://crm.hsa.gov.sg/event/feedback

HSA
Health Sciences Authority