Ethiopian Food and Drug Authority

Guidelines for Software as Medical Device and Artificial intelligence based medical device

First Edition

September 2022

Addis Ababa, Ethiopia

Table of Contents

ACRONYMS

AE	Adverse Event
AI	Artificial Intelligence
AI-MD	Artificial Intelligence Medical Device
COTS	Commercially-Off-the-Shelf
CSDT	Common Submission Dossier Template
CT	Computed Tomography
CVSS	Common Vulnerability Scoring System
EFDA	Ethiopian food and drug authority
EOL	End-Of-Life
eRIS	Electronic Regulatory Information System
EPSP	Essential Principles of Safety and Performance
FSCA	Field Safety Corrective Action
GUI	Graphical User Interface
ICD	Implantable Cardioverter-defibrillators
IMDRF	International medical device regulators forum
IOT	Internet Of Things
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
IT	Information Technology
IVD	In vitro diagnostics
LIS	Laboratory Information System
MD	Medical Device
OTS	Off-the Shelf

QMS	Quality Management System
SaMD	Software as a Medical Device
SBOM	Software Bill of Material
SOP	Standard Operating Procedure
TPLC	Total Product Life Cycle
PMS	Post market Surveillance

ACKNOWLEDGEMENT

The Ethiopian Food and Drug Authority (EFDA) would like to acknowledge and appreciate the Authority's Medical device technical working group members assigned to prepare this guideline for their invaluable contributions from its drafting to approval.

EFDA would also like to thank the Technical Advisors of partners who have been with the technical working group for the development of the document.

Last but not least, the Authority would like to extend its appreciation to the directors of relevant directorates who have encouraged and directed the experts in the working group by facilitating necessary resources until the completion of the document.

1 INTRODUCTION

The Food and Medicine Administration Proclamation (FMA) 1112/2019 mandates the Food and Drug Authority of Ethiopia (EFDA) to assess the safety, performance and quality of medical devices and give authorization for marketing of the devices in the country. Article 2 sub-article 22 of this Proclamation defines medical device as 'any instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, **software**, material or other similar or related articles and their accessories intended for medical use'. The scope of this definition and therefore the scope of the Authority's regulatory control includes non-physical medical devices (i.e. Software) that are intended for medical purpose.

Software is becoming increasingly important and pervasive in healthcare. Given the availability of a multitude of technology platforms as well as increasing ease of access and distribution, software created for medical purposes (software used to make clinical decisions) are being used in healthcare.

Existing regulatory requirements of the Authority address public health risks of software when embedded in hardware medical devices. However, it is equally important to set regulations and provide guidance to address the unique public health risks posed by Software as a Medical Device (SaMD) as well as assure an appropriate balance between patient/consumer protection and promotion of public health by facilitating innovation. 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).

This is therefore the document developed by the Authority to establish an appropriate framework to incorporate proper controls into the Authority's regulatory approaches for SaMD and Artificial Intelligence based medical devices (AI-MD). It is focused on a selected subset of medical device software called Software as a Medical Device.

Readers or users of this document can submit their feedbacks (specifically regarding the contents of this guidelines) to – Email: contactefda@efda.gov.et.

2 DEFINITIONS

Analytical / Technical validation:- measures the ability of a SaMD to accurately, reliably and precisely generate the intended technical output from the input data.

Artificial Inteligence (AI):- A set of technologies that seek to simulate human traits such as knowledge, reasoning, problem solving, perception, learning and planning.

Artificial Intelligence based Medical Device (AI-MD):- an artificial intelligence application intended to be used for medical purposes, such as investigation, detection, diagnosis, monitoring, treatment or management of any medical condition, disease, anatomy or physiological process.

Authority: - means Ethiopian food and drug authority

Clinical Evaluation:- The assessment and analysis of clinical data pertaining to a medical device to verify the clinical safety, performance and effectiveness of the device when used as intended by the manufacturer.

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.

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.

Software as a Medical Device (SaMD):- A software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device.

NB:

- SaMD is a medical device and includes in-vitro diagnostic (IVD) medical device.
- SaMD is capable of running on general purpose (non-medical purpose) computing platforms
- "without being part of" means software not necessary for a hardware medical device to achieve its intended medical purpose;
- Software does not meet the definition of SaMD if its intended purpose is to drive a

hardware medical device.

- SaMD may be used in combination (e.g., as a module) with other products including medical devices;
- SaMD may be interfaced with other medical devices, including hardware medical devices and other SaMD software, as well as general purpose software
- Mobile apps that meet the definition above are considered SaMD.

Valid clinical association: The extent to which the SaMD's output (concept, conclusion, measurements) is clinically accepted or well-founded (based on an established scientific framework or body of evidence), and corresponds accurately in the real world to the healthcare situation and condition identified in the SaMD definition statement. It also known as **scientific validity**.

3 SCOPE

This guideline applies to all SaMD that fall under the definition of Medical devices or In vitro diagnostic medical devices provided in FMA Proclamation 1112/2019 irrespective of software technology and/or platform. It is also applicable to all Medical devices incorporating Artificial Intelligence.

It is not applicable to-

- Software that are being used in healthcare for non-medical purpose (e.g., administrative, financial);
- Software used to make or maintain a device (testing, source code management, servicing, etc.)
- Software that are accessories to hardware medical devices (unless they meet the definition of SaMD); and
- Software in medical device (A software that is part of a device and is integral to the functioning of that device).

4 OBJECTIVE

The objective of this guideline is to provide clarity on the regulatory requirements for software as medical devices and AI based medical devices in their entire life cycle.

5 THE REGULATORY REQUIREMENTS FOR MARKETING AUTHORIZATION OF SaMD

5.1 General

The Authority is responsible to ensure a high level of protection of public health and safety. As one of its major functions, it evaluates the evidences generated and submitted by the manufacturers of medical devices to demonstrate that their products are in compliance with all applicable regulatory requirements. The conformity assessments from which such evidences are generated, conducted before and after a medical device is placed on the market, are complementary elements of the medical device regulatory system in the Authority. The conformity assessments of Medical devices including SaMD are intended to provide the objective evidence of safety, performance, and benefits and risks to maintain public confidence in the product.

Manufacturers of all classes of medical devices including SaMD are expected to demonstrate conformity of the device to the Essential Principles of Safety and Performance of Medical Devices through the preparation and holding of technical documentation that shows how each medical device was developed, designed and manufactured together with the descriptions and explanations necessary to understand the manufacturer's determination with respect to such conformity. The extent of evidence included in the technical documentation is expected to increase with the class of the medical device, its complexity, and the extent to which it incorporates new technology.

5.2 Technical Requirements

As part of its activities of conformity assessment outputs evaluation, the Authority developed and is using two guidelines for the registration requirements of the two groups of medical devices (In vitro diagnostics and Non In vitro diagnostics). The following requirements are extracted from different sections of both guidelines as they are also applicable and required for SaMD.

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

These topics and other important guidances are provided in detail in the subsequent sections of this document.

6 RISK MANAGEMENT FOR SaMD

Risk management should review and address all foreseeable risks and failure modes of the software in its product life cycle. Risk assessment and evaluation should commensurate with the complexity and risk classification assigned to the SaMD 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 to:

i. identify all possible hazards,
ii. assess the associated risks,
iii. implement mitigation or control measures to reduce risks to acceptable level and
iv. observe and evaluate effectiveness of mitigation measures.

Where there are changes made to a SaMD, 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.

This section of the document is not intended to replace or create new risk management practices rather it uses risk management principles in the ISO 14971 to identify generic risks for SaMD. The four categories (Category I, II, III and IV) that are described in this document are not to replace or conflict with the content of risk-based classification of IVD and Non-IVD medical devices provided in other guidelines of the Authority.

6.1 SaMD Aspects Influencing Patient Safety

There are many aspects in an ever-increasing complex clinical use environment that can raise or lower the potential to create hazardous situations to patients. Some examples of these aspects include:

- The type of disease or condition
- Fragility of the patient with respect to the disease or condition
- Progression of the disease or the stage of the disease/condition
- Usability of the application
- Designed towards a specific user type
- Level of dependence or reliance by the user upon the output information
- Ability of the user to detect an erroneous output information
- Transparency of the inputs, outputs and methods to the user
- Level of clinical evidence available and the confidence on the evidence
- The type of output information and the level of influence on the clinical intervention
- Complexity of the clinical model used to derive the output information
- Known specificity of the output information
- Maturity of clinical basis of the software and confidence in the output
- Benefit of the output information vs. baseline
- Technological characteristics of the platform the software are intended to operate on.
- Method of distribution of the software

Generally, these aspects can be grouped into the following two major factors that provide adequate description of the intended use of SaMD:

(i) Significance of the information provided by the SaMD to the healthcare decision, and

(ii) State of the healthcare situation or condition.

When these factors are included in the manufacturer's description of intended use, they can be used to categorize SaMD.

6.2 Factors Important for SaMD Characterization

6.2.1 Significance of information provided by SaMD to healthcare decision

The intended use of the information provided by SaMD in clinical management has different significance on the action taken by the user.

6.2.1.1 To treat or to diagnose

Treating and diagnosing infers that the information provided by the SaMD will be used to take an immediate or near term action:

- To treat/prevent or mitigate by connecting to other medical devices, medicinal products, general purpose actuators or other means of providing therapy to a human body.
- To diagnose/screen/detect a disease or condition (i.e., using sensors, data, or other information from other hardware or software devices, pertaining to a disease or condition).

6.2.1.2 To drive clinical management

Driving clinical management infers that the information provided by the SaMD will be used to aid in treatment, aid in diagnoses, to triage or identify early signs of a disease or condition will be used to guide next diagnostics or next treatment interventions.

6.2.1.3 To Inform clinical management

Informing clinical management infers that the information provided by the SaMD will not trigger an immediate or near term action:

- To inform of options for treating, diagnosing, preventing, or mitigating a disease or condition.

- To provide clinical information by aggregating relevant information (e.g., disease, condition, drugs, medical devices, population, etc.).

6.2.2 Healthcare Situation or Condition

6.2.2.1 Critical situation or condition

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. SaMD is considered to be used in a critical situation or condition where:

- The type of disease or condition is:
    - Life-threatening state of health, including incurable states,
    - Requires major therapeutic interventions,
    - Sometimes time critical, depending on the progression of the disease or condition that could affect the user's ability to reflect on the output information.
- Intended target population is fragile with respect to the disease or condition (e.g., pediatrics, high risk population, etc.)

6.2.2.2 Serious situation or condition

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. SaMD is considered to be used in a serious situation or condition when:

- The type of disease or condition is:
    - Moderate in progression, often curable,

- Does not require major therapeutic interventions,
- Intervention is normally not expected to be time critical in order to avoid death, long-term disability or other serious deterioration of health, whereby providing the user an ability to detect erroneous recommendations.

- Intended target population is NOT fragile with respect to the disease or condition.

6.2.2.3 Non-Serious situation or condition

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. SaMD is considered to be used in a non-serious situation or condition when:

- The type of disease or condition is:
  - Slow with predictable progression of disease state (may include minor chronic illnesses or states),
  - May not be curable; can be managed effectively,
  - Requires only minor therapeutic interventions, and
  - Interventions are normally noninvasive in nature, providing the user ability to detect erroneous recommendations.

- Intended target population is individuals who may not always be patients.

6.3 Risk Categories of SaMD

6.3.1 SaMD Categorization Principles

This subsection of the document provides risk categories of SaMD based on the factors provided in sub-section 6.2. This categorization principle is not intended to replace or create new classification of medical devices required in other documents of the Authority. The determination

of the categories is the combination of the significance of the information provided by the SaMD to the healthcare decision and the healthcare situation or condition.

The four categories (I, II, III, IV) are based on the levels of impact on the patient or public health where accurate information provided by the SaMD to treat or diagnose, drive or inform clinical management is vital to avoid death, long-term disability or other serious deterioration of health, mitigating public health. The categories are in relative significance to each other. Category IV has the highest level of impact, Category I, the lowest.

6.3.2 SaMD Categories

Table 1: Categories of Software as Medical device

State of Healthcare situation or condition	Significance of information provided by SaMD to healthcare decision		
	Treat or Diagnose	Drive Clinical Management	Inform Clinical Management
Critical	IV	III	II
Serious	III	II	I
Non-Serious	II	I	I

7 QUALITY MANAGEMENT SYSTEM FOR SaMD

All manufacturers of medical devices, including SaMD should have a QMS in place to ensure manufacturing quality and consistency in the product's specification as it is required by the Authority's Guidelines for Medical device Good Manufacturing Practices (GMP). The principles given in the GMP Guidelines that provide structure and support to the lifecycle processes and activities are still applicable and important to control the quality of SaMD.

An effective QMS for SaMD should include the following principles:

- **Leadership and an organizational structure**- that provides leadership, accountability, and governance with adequate resources to assure the safety, effectiveness, and performance of SaMD;

- **A set of life cycle supported processes-** 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 SaMD product realization activities.

- **Product realization 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

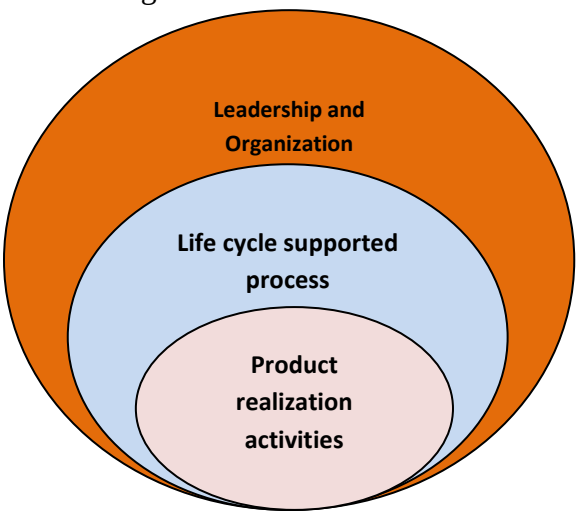

Figure 1: Quality Management Principles

a) Leadership and an organizational structure

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

Management of the organization 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 SaMD. In addition, top management should ensure the availability and appropriate level of resources to ensure the effectiveness of the SaMD. The resources include:- people, infrastructure, environment, tools etc. It is also important to ensure people who are assigned to the SaMD projects are competent and equipped with adequate skillsets, experience and training.

b) Life cycle supported processes

The life cycle supported processes refers to the important processes that support the SaMD 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 SaMD life cycle and should take a risk-based approach to patients safety. Software risk management requires a balance 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** –a configuration management plan should be established to systematically manage and control configurable items (e.g. source codes, documents, release versions, software tools and etc.) throughout the SaMD life cycle. This is necessary to maintain integrity and traceability of the software configurations throughout its life cycle and also to ensure correct installation and integration of the SaMD in the clinical setting.

- **Measurement, Analysis and Improvement** – The effectiveness of the software life cycle processes and of the software itself should be evaluated based on predetermined procedures to collect and analyse appropriate data. 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 organization should ensure control over such outsourced processes. When a commercial-off-the-shelf (COTS) software is chosen, used or integrated into the SaMD, the product owner of the SaMD is ultimately responsible for its safety and performance.

c) Product Realization Activities

Product realization activities forms the inner core activities of the QMS principles. It is supported by the outer cores: Leaderships & Organizations and the Life Cycle Supported Processes. 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.

An example of product realization activities which are commonly found in software engineering life cycle approach are shown in Figure 2 below. The product realization activities mentioned here should be methodology (e.g. Waterfall, Agile, or V-model) agnostic.

Figure 2: Example of a typical software engineering life cycle approach for product realization

- **Defining Requirements** – requirements captured must be in line with the intended use of the software as 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 as medical device. Various clinical settings and home use environments where the SaMD 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** – Verification provides assurance that the design and development activities at each development stage conforms to the requirements, while Validation provides reasonable confidence that the SaMD 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 SaMD 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.

- **Decommissioning** – activities to terminate maintenance, support and distribution of the SaMD, in a controlled 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).

8 ESSENTIAL PRINCIPLES FOR SAFETY AND PERFORMANCE OF SaMD

All medical devices including SaMD 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 SaMD must be identified and where requirements are deemed not applicable, the rationale has to be documented. This applies to all Classes of SaMD.

Applicants may refer to relevant sections of the Authority's *General Guidelines for Marketing Authorization of medical device* and Annexes of the *Guidelines for Registration Requirements of Non-IVD Medical devices* and *Guidelines for Registration Requirements of IVD Medical devices* to have better understanding of the required EPSP.

The essential design and manufacturing principles that may be relevant to SaMD are listed below in Table 2.

Table 2: Essential design and manufacturing principles

Essential design and manufacturing principles	**Applicability to SaMD**
Essential Principles applicable to medical devices and IVD medical devices	
General requirements	√
Clinical Evaluation	√
Chemical, physical and biological properties	
Sterility, packaging and microbial contamination	
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	
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	
Performance Characteristics	√

The manufacturers of SaMD should generate the required and relevant evidences to demonstrate that their SaMD complies with all the applicable EPSPs.

8.1 Clinical Evaluation

Clinical evaluation of SaMDs 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 manufacturer's intended use.

A valid clinical association is an indicator of the level of clinical acceptance and how much meaning and confidence can be assigned to the clinical significance of the SaMD's output in the intended healthcare situation and the clinical condition/physiological state.

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

- Referencing existing literature and well-established clinical guidelines;
- Comparison with similarly established SaMD and other non-SaMD 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 as 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.

It is important to note that clinical evaluation should be an on-going process throughout the software life cycle. After the software as medical device has been deployed in the market, 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.

8.2 Labelling Requirements

Device labelling (e.g. physical label, instructions for use, implementation manual etc.) serves to help users:

a) identify the device and its Manufacturer;

b) to communicate safety and performance related information; and

c) 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.

SaMD 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 categorized into two groups based on the mode of supply:

a) supplied in physical form or

b) supplied without a physical form.

8.3 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 should be required during the registration process.

In addition, information on the software version being registered in Ethiopia is to be clearly presented on the device labelling (if supplied in physical form) or software graphical interface (if supplied without physical form), depending on the mode of supply of the software. The software version information that represents all software changes/iteration (e.g. graphic interface, functionality, bug fixes) has to be provided to the Authority. This does not include Software version numbering that is solely for testing or internal use only (e.g. checking in of source code).

8.4 Design Verification & Validation

SaMDs should be designed to ensure accuracy, reliability, precision, safety and performance, while fulfilling their intended use. Analytical validation is the process of generating objective evidence to support the safety and performance of the SaMD.

As discussed in section 7(c) under "Product realization activities" above, analytical validation of SaMD(s) generally performed during the verification and validation phase of the software development life cycle. The software verification process ensures that software specifications are met, by demonstrating that the design inputs generate 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.

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 need 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.

8.5 Cybersecurity

Minimum necessary requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorized 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 product registration:

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

ii. Cybersecurity vulnerabilities (known and foreseeable), risk analysis focusing on assessing the risk of patient harm 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.

iv. Evidence that the security of the device/ effectiveness of the security controls have been verified. It should contain the following information where applicable:

    a. Descriptions of test methods, results, and conclusions;

b. A traceability matrix between security risks, security controls, and testing to verify those controls; and

c. References to any standards and internal SOPs/documentation used.

8.5.1 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 SaMDs 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 SaMD.

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.

8.5.2 Cybersecurity Considerations

When developing a SaMD, a cybersecurity plan should be devised to include the following considerations but not limited to:

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

8.5.2.1 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.

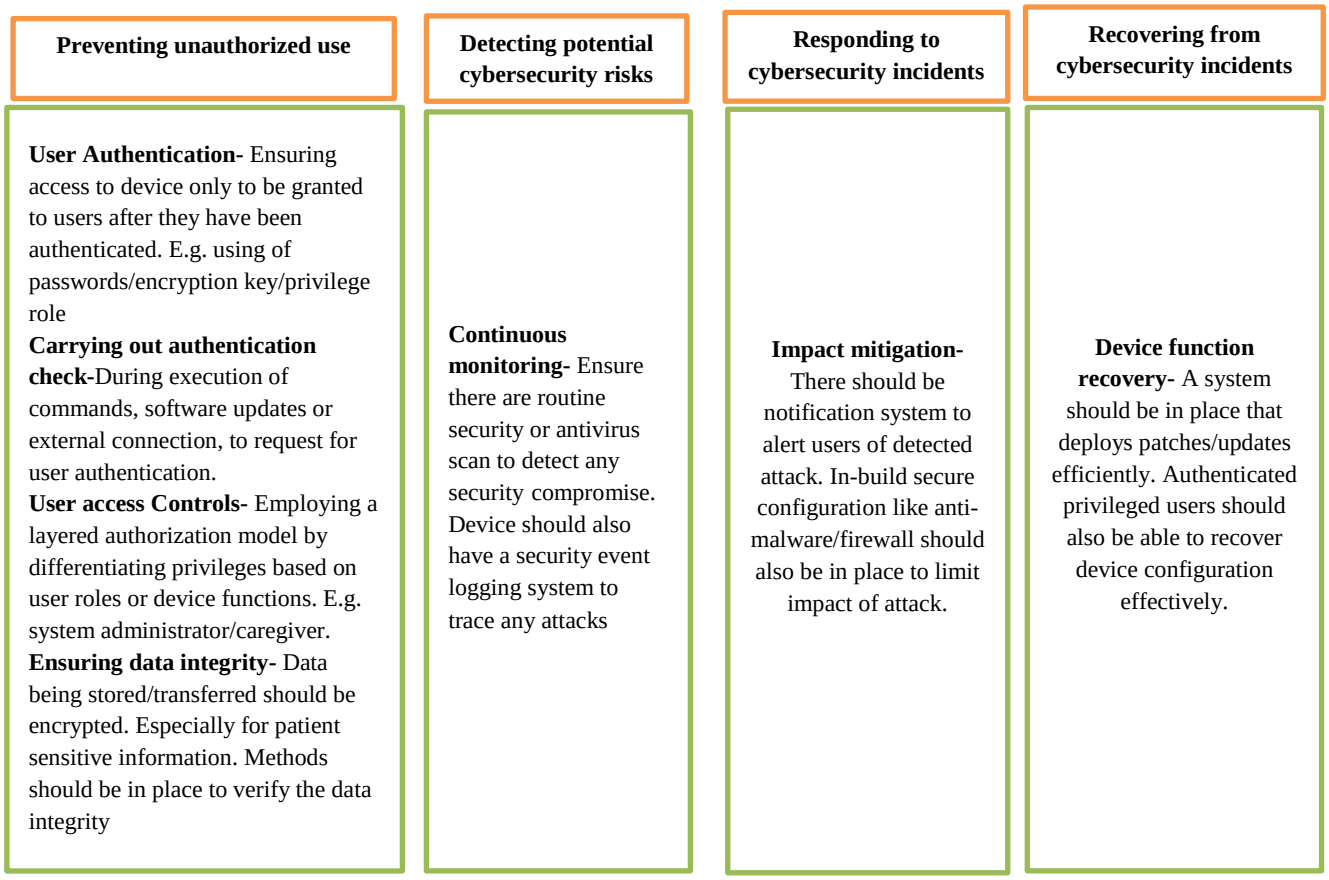

Figure 3: Cybersecurity design considerations (non-exhaustive)

8.5.2.2 Customer Security Documentation

Besides supplying the end users with the Instructions for use (IFU) on the appropriate usage of the SaMD, manufacturers should also consider providing a customer security documentation to communicate the relevant security information to mitigate cybersecurity risks when operating the SaMD 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 SaMD

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 unauthorized 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.

Since the above mentioned information (e.g. SBOM) may reveal sensitive information about the strengths and weaknesses of a SaMD cybersecurity, it is recommended that the manufacturer determines an appropriate communication channel to securely distribute such information.

8.5.2.3 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 can be achieved by using established vulnerability scoring methodology such as the Common Vulnerability Scoring System (CVSS). Additionally, this assessment should consider the existing compensating controls and mitigating measures to determine if the overall cybersecurity risk involved is of acceptable or unacceptable residual risk. If it is deemed that additional mitigating measures or compensating controls are required to mitigate the risk, manufacturer shall practice 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.

8.5.2.4 Verification and Validation of Cybersecurity risk control measures

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.

8.5.2.5 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 SaMDs 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 in the Table 3 below.

Table 3: Cybersecurity post-market planning

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.

8.5.3 Patient Confidentiality and Privacy

Medical device cybersecurity incidents can affect patient safety and privacy. There are increasing reports of breaches of data privacy. SaMD 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. It is the responsibility of the manufacturers, importers and distributors to ensure that the SaMD meets the requirements of any other applicable regulatory controls in Ethiopia.

9 ARTIFICIAL INTELLIGENCE BASED MEDICAL DEVICES (AI-MD)

This section presents some additional regulatory considerations specific to medical devices incorporating Artificial Intelligence (AI) technology. This includes AI applications with medical purpose that is incorporated into a hardware medical device.

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 national legislation and regulatory requirements applicable to the development and deployment of AI-MD in healthcare should be complied with.

9.1 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 based on medical device quality management system.

The following additional information (Table 4) should be submitted for pre-market registration of AI-MDs.

Table 4: Additional considerations for product registration for AI-MD

Requirement	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. 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 presented. Please refer to Section 3.5 for more information.

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 the Authority. 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.

9.2 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, on-going 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 4 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,

software 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.

10 SOFTWARE WITH MULTIPLE FUNCTIONS

SaMDs typically contain multiple functions, some of which may not fall under the definition of a medical device indicated in Food and Medicine Administration Proclamation No. 1112/2019. Such non-MD functions may include the following:

- Software function that allows storing, converting formats or transferring patient data;
- Software function that is intended to provide general patient education and facilitate access to commonly reference information;
- Software function that allows automation of general office operations (e.g. patient scheduling, billing and etc.) in a healthcare setting.

With regard to the provision of information/validation for such non-MD functions, applicants are not required to submit them during registration. However, the manufacturers are still required to consider if the non-MD functions will impact the 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 and etc.). The manufacturer is expected to analyse and mitigate the risk to an acceptable level and the appropriate verification/validation should be performed to ensure mitigation effectiveness. These risk management process including the assessment/actions shall be documented as part of the manufacturer's quality management system.

11 SaMD MANUFACTURERS AND DISTRIBUTORS

All manufacturers, importers and wholesalers of SaMDs shall hold medical device license for the respective activities they perform as per Medicine and Medical Device Import, Export and

Wholesale Directive of the Authority. The pre-requisite for licensing is to implement and maintain an appropriate quality management system (QMS) which covers the following aspects:

- Ensure the software is developed and manufactured under an appropriate and effective quality management system (e.g. ISO 13485).
- Ensure traceability of the SaMD. 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 life cycle of the software.

An Individual or a company who wants to develop or manufacture and market SaMD in the country should apply and be issued a manufacturing license by the Authority after complying with the requirements set in the related regulatory documents.

12 CHANGES TO A REGISTERED SaMD

A SaMD 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, the Authority employs a risk-based approach to manage the changes to registered software; the regulatory requirements of the change commensurate with the significance of the change. For instance, significant 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.

Non-significant software changes are required to be notified to the Authority. Such notification changes may be bundled in a change notification application.

The applicant are advised to follow Guideline for Medical device Post-approval Change Notification of the authority when applying changes to the registered software as a medical devices before being implemented by the manufacturer.

13 POST-MARKET MANAGEMENT OF SaMD

13.1 PMS for all SaMDs

Post-market monitoring and surveillance of SaMDs 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 SaMDs in Ethiopia (manufacturers, importers and wholesalers) are required to comply with their post-market duties and obligations which includes reporting of device defects or malfunctions, recalls, FSCAs 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 SaMDs.

13.2 PMS for AI-MDs

Once AI-MDs are deployed in the real-world environment, active monitoring, review and tuning are necessary. Manufacturers and Importers 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 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. The developer should apply appropriate control measures based on the findings after deployment.

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

13.3 Field Safety Corrective Actions (FSCA)

With the increasing usage of software in healthcare delivery systems it is expected that the number of software issues affecting the service 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 manufacturer 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 manufacturer should initiate a FSCA to communicate the risks to users and inform of the measures to be implemented to mitigate the risks.

Examples of SaMD issues that may require FSCA:

- Inaccurate or incorrect test results e.g. mixed up of patient results and demographics
- Wrong classification of disease types. Eg. wrong classification of malignant lesion as a benign lesion.
- Potential clinical misdiagnosis and/or mistreatment e.g. uploading of incorrect treatment plan during exportation
- 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

Software errors may be introduced during design and development of the device and also during use of the device. The following lists are 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 third-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.

13.4 Adverse Events

As part of the post-market duties and obligations, companies involved in distributing medical devices in Ethiopia (manufacturers, importers and wholesalers) are required to report Adverse Events (AE) associated with the use of SaMDs. 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 SaMDs may directly or indirectly, have an impact on patients and users. 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, 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 SaMDs may arise due to but not limited to:

- 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

14 References

1. *Regulatory Guidelines for Software Medical device – A Lifecycle Approach, V 2. Health Sciences Authority of Singapore, April 2022.*
2. *Proclamation No.1112/2019: Proclamation to provide for food and medicines administration, 2019*
3. *Software as a Medical Device (SaMD): Clinical Evaluation. IMDRF/SaMD WG/N41FINAL:2017, International Medical Device Regulator Forum(IMDRF), 21 September 2017.*
4. *Software as a Medical Device (SaMD): Application of Quality Management System. IMDRF/SaMD WG/N23 FINAL: 2015, International Medical Device Regulator Forum(IMDRF), 2 October 2015.*
5. *Software as a Medical Device (SaMD): Key Definitions. IMDRF/SaMD WG/N10FINAL:2013, International Medical Device Regulator Forum(IMDRF), 9 December 2013.*
6. *"Software as a Medical Device": Possible Framework for Risk Categorization and Corresponding Considerations. IMDRF/SaMD WG/N12FINAL:2014, International Medical Device Regulator Forum (IMDRF), 18 September 2014.*
7. *Medical device software – Software life cycle processes. International Standards. IEC 62304, 1st Edition, 2006-05.*
8. *Medical devices- Quality management systems-Requirements for regulatory purposes. ISO 13485: 2016.*
9. *Medical devices- Application of risk management to medical devices. ISO 14971: 2019.*