HPT/PER/GUD/099

Revision :0

MINISTRY OF HEALTH

PHARMACY AND POISONS BOARD

GUIDELINE ON REGULATION OF MEDICAL DEVICE SOFTWARE IN KENYA (MDSW)

FEBRUARY, 2026

Citation of this Document

The author of this document is the Pharmacy and Poisons Board, a State Corporation under the Ministry of Health, Republic of Kenya. It may be reproduced or adopted on the condition that the recommended citation below is made.

Recommended citation: Republic of Kenya, Ministry of Health, Pharmacy and Poisons Board, Guideline on Regulation of Medical Device Software in Kenya Version 0, 2026

For clarifications, comments, or suggestions, please contact:

The Chief Executive Officer
Pharmacy and Poisons Board
P.O. Box 27663 – 00506, Nairobi
Telephone: 0709770100
Email: info@ppb.go.ke
Website: webmaster@ppb.go.ke

Prepared by Head, Medical Devices and In-Vitro Diagnostics

Name..PAULYNE WAIRIMU.....

Sign.....

Date..8th- April- 2026.....

Reviewed by: Director, Health Products and Technologies

Name..Ali Abdullahi Arale.....

Sign.....

Date..9th April 2026.....

Checked by Head, Quality Management

Name..ANTHONY KEMBOI.....

Sign.....

Date..09/04/2026.....

Authorized by Chief Executive Officer

Name..Dr. AHMED I. MOHAMED.....

Sign.....

Date..09/04/2026.....

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS

AE	Adverse Effect
AI	Artificial Intelligence
CDS	Clinical Decision Support
CSTD	Common Submission Dossier Template
CVSS	Common Vulnerability Scoring System
DICOM	Digital Imaging and Communication in Medicine
ECG	Electrocardiogram
EEG	Electroencephalogram
FSCA	Field safety corrective actions
GDPR	General Data Protection Regulation
GMLP	Good Machine Learning Practices
HCP	Health Care Providers
IEC	International Electrotechnical Commission
IFU	Instructions for Use
IMDRF	International Medical Devices Regulators Forum
IVD-MD	In-Vitro Diagnostics Medical Device
LAR	Local Authorized Representative
LM	Legal Manufacturer
MA	Marketing Authorization
MD	Medical Device
MDSW	Medical Device Software
ML	Machine Learning
PDS	Patient Decision Software
PI	Product Identifier
PV	Pharmacovigilance
SaMD	Software as a Medical Device
SiMD	Software in a Medical Device

SRS	Software Requirement Specification
UDI	Unique Device Identifier
US FDA	US Food and Drug Administration
WHO	World Health Organization

GLOSSARY OF TERMS

Software;

For the purpose of this guidance, "software" is defined as a set of instructions that processes input data and creates output data.

Input data;

- Any data provided to software in order to obtain output data after computation of this data can be considered as input data. Input data examples (non-exhaustive):
- Data given through the use of a human data-input device such as a keyboard, mouse, stylus, or touch screen;
- Data given through speech recognition;
- Digital document: formatted for general purpose such as Word file or pdf file or jpeg image, formatted for medical purpose such as DICOM file or ECG records or Electronic Health Record, unformatted document. Note that digital documents have to be differentiated from software able to read such documents;
- Data received from/transmitted by devices.

Output data

- Any data produced by a software can be considered as an output data. Output data examples (non- exhaustive):
- Screen display data (such as layout with number, characters, picture, graphics, etc.);
- Print data (such as layout with number, characters, picture, graphics, etc.);
- Audio data;
- Digital document (formatted for a general purpose such as Word file or pdf file or jpeg image, or formatted for medical purpose such as DICOM file or ECG records or Electronic Health Record, unformatted document).
- Haptic buzzing as an alternative to audio sound
- instruction to a human user or in control of another device [1]

[1] (European Commission-Medical Device Coordination Group, 2019)

Medical Device Software

Medical device software (MDSW) refers to software intended for use in healthcare, alone or in combination with hardware, to diagnose, treat, or monitor a medical condition. This includes software that is an integral part of a medical device (SiMD) or standalone software used for medical purposes (SaMD)[2].

SaMD is defined as a software intended to be used for one or more medical purposes that perform these purposes without necessarily being part of a hardware medical device.

SiMD is defined as software that is part of a hardware Medical Device.

Aware of the evolving technology, the term SaMD has also changed to reflect a more diverse landscape of software and varied interpretation across jurisdictions. As such, considerations for any software that meets the definition of a medical device (SaMD) or is part of a medical device (SiMD) have been made.

This guidance document refers to these set of software as 'medical device software' that include the below listed interpretations;

a) is intended to generate information for use in achieving one or more medical purposes;
b) is part of a hardware medical device;
c) is not part of a hardware medical device and is independent of other medical devices;
d) is necessary for a medical device to achieve its intended use/intended purpose;
e) is driven or influenced by another medical device;
f) has an output intended for a human user, medical device, and/or non-medical device; and
g) uses inputs from humans, medical devices, and/or products that are not medical devices.

Medical device software can operate in complex socio-technical environments consisting of:

[2] https://www.fda.gov/medical-devices/digital-health-center-excellence/digital-health-terms. (USFDA, 2022)

- software,
- hardware,
- networking, and
- people

which form a complex and dynamic interaction between the software function, its inputs and outputs, the intended user, patient and the unique healthcare circumstances in which the software is used. This complexity together with:

- the interconnectedness of systems,
- the need for cybersecurity,
- the speed and frequency of development cycles,
- the speed at which a solution can be scaled up, and
- the various aspects of change implementation
- level of expertise of the User(s) to offer human oversight
- readiness of the healthcare system

contribute to the accurate depiction of a device and/or its risk profile. Medical device software can pose risks that are distinct and unique, such as those that relate to the information that is generated, output by the device and the capacity for varied degrees of autonomy. This medical device software may be used independently or as part of a platform and span a wide spectrum of risk profiles depending on the intended use, and potential harms associated with use and/or inaccurate outputs.[3]

Reference is made to **Annex I**, with examples of regulated medical device software, and what is not considered as a medical device software.

Platform

A platform would refer to the software environment, framework or operating system that support development, deployment or execution of medical device software, such as operating systems, cloud or data platforms.

Software Function

Software function in a medical device software is a specific, discrete action or operation performed by the software to achieve a defined purpose that contributes to the overall devices intended medical use. It is the smallest unit

[3] (IMDRF:Software as a Medical Device Working Group, 2025)

of software behaviour that can be individually specified, designed, tested and traced to a use need or system requirement

Module

Modules refers to a discreet identifiable and self-contained unit of software, that performs a specific task, or set of tasks within the overall software system.

Software Item

Software Item: This is well defined identifiable component of the software system that performs a specific function *or set* of functions

Software system:

Software System refers to the complete integrated set of components that work together to achieve the intended function of a medical device, this may include both hardware and software elements as well as any external interfaces

Medical Device

'Medical device' means any instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings, for one or more of the specific medical purpose(s) of:

- diagnosis, prevention, monitoring, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury,
- investigation, replacement, modification, or support of the anatomy or of a physiological process,
- supporting or sustaining life,
- control of conception,
- disinfection of medical devices,
- providing information by means of in vitro examination of specimens derived from the human body; and does not achieve its primary intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its intended function by such means.

Note: Products which may be considered to be medical devices in some jurisdictions but not in others include:

- disinfection substances,
- aids for persons with disabilities,
- devices incorporating animal and/or human tissues,
- devices for in-vitro fertilization or assisted reproduction technologies.

In Vitro Diagnostic (IVD) medical device

'In Vitro Diagnostic (IVD) medical device' means a medical device, whether used alone or in combination, intended by the manufacturer for the in-vitro examination of specimens derived from the human body solely or principally to provide information for diagnostic, monitoring or compatibility purposes.

IVD medical devices include reagents, calibrators, control materials, specimen receptacles, software, and related instruments or apparatus or other articles and are used, for example, for the following test purposes: diagnosis, aid to diagnosis, screening, monitoring, predisposition, prognosis, prediction, determination of physiological status.

Intended use / intended purpose

The term "intended use / intended purpose" is the objective intent of the manufacturer regarding the use of a product for delivering the medical purpose, process or service as reflected in the specifications, instructions and information provided by the manufacturer.[4]

A Medical Purpose - in the context of a Software as a Medical Device, as in the context of this document-refers to a SaMD that is;

- Intended to acquire, process, or analyse a medical image, or a signal from an in vitro diagnostic device or a pattern/signal from a signal acquisition system or imaging device, OR
- Intended for the purpose of supporting or providing recommendations to health care professionals, patients or non-healthcare professional caregivers about prevention, diagnosis, treatment, or mitigation of a disease or condition. [5] Software that fits the above criteria can be

[4] (GHTF-Label and Instructions for Use for Medical Devices, 2011)
[5] (Health Canada, 2019)

broadly categorized under the terms Clinical Decision Support Software (CDS) and Patient Decision Support Software (PDS). CDS software (intended for Health Care Providers (HCP)), and PDS software (intended for patients and caregivers who are not HCPs) can encompass a wide spectrum of software functionalities.

- Not all medical software have a medical purpose and require regulations. **Annex I** provide examples of software that do not meet the requirements for regulation.

Artificial Intelligence (AI) - A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action [6]

Machine Learning (ML): A set of techniques that can be used to train AI algorithms to improve performance at a task based on data[7]

Conformity Assessment: The process of evaluating whether an MDSW meets regulatory requirements, including technical documentation, clinical evaluation, and quality management system (QMS) compliance.

Clinical Evaluation: A systematic process to assess the safety and performance of MDSW based on clinical data, ensuring it meets its intended purpose without undue risk.

Quality Management System (QMS): A formalized system (e.g., ISO 13485) that ensures consistent design, development, and maintenance of MDSW to meet regulatory and safety standards.

Post-Market Surveillance (PMS): Ongoing monitoring of an MDSW after-market release to ensure continued safety and performance, including reporting adverse events and updates.

[6] (Removing Barriers to American Leadership in Artificial Intelligence, 2025)
[7] (Us Government-Office of the President Federal Register, 2023)Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Sec. 3(b)

Software life cycle process: An international standard for the software life cycle processes of medical device software, covering development, maintenance, and risk management such as IEC 62304.

Risk Management: The process of identifying, evaluating, and mitigating risks associated with MDSW, as required by standards like ISO 14971.

Significant Change: Change(s) that could reasonably be expected to affect the safety, quality and performance of a registered MDSW

ACKNOWLEDGEMENTS

The Pharmacy and Poisons Board extends its sincere gratitude to all who contributed to the development of this guideline on Medical Devices Software We express our profound appreciation to the Cabinet Secretary for Health, Hon. Aden Duale Bare EGH, MP, for his unwavering support and vision.

Our heartfelt thanks go to the Principal Secretary of the Ministry of Health Hon. Mary Muthoni Muriuki CBS, HSC, State department for public health and professional for her invaluable guidance and leadership.

We are deeply grateful to the Acting CEO Dr. Ahmed Mohamed at the Pharmacy and Poisons Board, for his dedication and commitment to advancing healthcare technology regulation.

We also acknowledge the vital contributions of industry stakeholders and partners; whose expertise and insights were instrumental in shaping this document.

We also acknowledge the contribution done by US-FDA Center for Devices and Radiological Health (CDRH), and Health Canada, whose support has been indispensable. We acknowledge the support of the USFDA and Health Canada as the Co-chairs of the IMDRF SAMD working group.

We also acknowledge the contribution of the African Union Development Agency, Medicines policy and regulatory reforms technical committee on the input particularly to the addition of the AU Model law harmonization.

Special recognition is extended to the Gates Foundation (GF) for their technical inputs and funding, which made this initiative possible.

FOREWORD

The Pharmacy and Poisons Board, under the Ministry of Health, Republic of Kenya, presents this guideline on Medical Device Software (MDSW). This document aims to provide clarity and direction for the regulation of Medical Device Software which includes Software as a medical device (SaMD) and Software in a medical device (SiMD) reflecting the evolving landscape of healthcare technology.

This Guideline is developed in response to the increasing prevalence and complexity of software used for medical purposes, recognizing the unique public health benefits and risks associated with MDSW. It delineates Software as Medical Device (SaMD) from Software in a Medical Device (SiMD) and outlines the regulatory requirements for ensuring quality, safety and performance.

This Guideline seeks to foster innovation, enhance patient safety, and improve accessibility to healthcare through advanced technologies. By providing a robust regulatory framework, it aims to streamline approval pathways for Medical Device Software, address ethical considerations, and ensure interoperability with other digital health tools.

This Guideline will serve as a valuable resource for manufacturers, healthcare providers, patients and caregivers, contributing to the advancement of healthcare in Kenya.

1.0 INTRODUCTION

1.1 Background

The Pharmacy and Poisons Board (PPB) is the National Regulatory Authority established under the Pharmacy and Poisons Act, Cap 244 of the Laws of Kenya, to regulate the profession of pharmacy and ensure the safety, quality and efficacy/perfomance of health products and health technologies including medical devices and *In-vitro* diagnostics.

The guidelines on submission of documentation for registration of medical devices including in-Vitro Diagnostics (IVD's) PPB/PER/MDV/GUD/011 has made provisions for the requirements for documentation requisite for applying for registration. However, the need to define further the context of a software as a medical device to adequately address the unique public health risks posed by this group of devices, and separate the requirements from those of a software that is embedded in a medical device, which have been traditionally considered has led to the need to develop this guidance document.

Software that is intended to be used for medical purposes without being part of a hardware medical device is referred to as "Software as a Medical Device (SaMD)". In this context, the SaMD performs one or more medical functions that includes, diagnosis, prevention, monitoring, treatment or alleviation of diseases.

MDSW is subject to regulatory oversight to ensure quality, safety, and performance based on the risk classification of the Medical Device. The use of MDSW provides easier access to advanced technologies for patients, therefore enhancing accessibility to healthcare. These advanced technologies can include Artificial intelligence (AI) and machine learning, related to SaMD, which can improve patient outcomes. MDSW represents a transformative shift in healthcare, offering new ways to diagnose, treat, and manage medical conditions and access to patients including those in remote settings.

To keep abreast with the ever-evolving technological advancement in health, developing this guidance document will ensure patient safety through robust regulatory oversight, promote innovation by streamlining the approval pathways for MDSW, enhance the interoperability with electronic health records and other digital health tools. Additionally, this guidance document will address ethical concerns such as biases in Artificial intelligence algorithms and data privacy.

Regulation of Medical Devices Software (MDSW) in Kenya shall be anchored in a harmonised application of the WHO Cybersecurity Framework, the Kenya National Cybersecurity Strategy (2022–2027), and the Kenya AI Strategy (2025–2030). This integrated approach recognises that software-driven and AI-enabled medical technologies are essential to patient safety, health system resilience, and national digital transformation. In line with WHO guidance, MDSW regulation shall require clear cybersecurity governance and leadership, with defined roles and accountability across manufacturers, deployers, healthcare institutions, and regulators. This aligns with Kenya's national cybersecurity governance structures and reinforces cybersecurity as a shared responsibility across the digital health ecosystem.

The classification of MDSW is crucial for determining the level of regulatory oversight required. This classification is generally based on the intended use of the MDSW and the potential risk it poses to patients. The International Medical Device Regulators Forum (IMDRF) has provided a framework that helps in classifying MDSW, which can be adapted for regulatory purposes in Kenya.

1.2 Legal Framework

The PPB is empowered under Section 3A(a) of the Pharmacy and Poisons Act ("the Act") to formulate guidelines for regulating the manufacture, import and export, distribution, sale and use of medical products including medical devices and IVDs.

Further, the Board is empowered under Section 3A of the Act to grant or withdraw marketing authorization for medical devices and IVDs subject to appropriate conditions and revise such conditions for marketing authorization as necessary.

This guideline is intended to implement the requirements of the Act stipulated under Section 3B(2)(b) to ensure that all medicinal products manufactured in, imported into or exported from the country conform to prescribed standards of quality, safety and performance. In doing so, Section 3B(2)(i) of the Act requires the Board to consider applications for approval and alterations of dossiers intended for use in marketing authorization of medicinal substances.

In performing its regulatory functions, the PPB is empowered under Section (3B(2)(r) of the Act to collaborate with other national, regional and international institutions on medical substances regulation. This enables the Board to recognize and rely on registrations and certifications from notified bodies and listed reference regulatory authorities. The Board remains independent, responsible and accountable for the decisions taken, even when it relies on the decisions, assessments and information of others.

The Health Act 2017, The Pharmacy and Poisons (*Registration of Health Products and Technologies*) Rules of 2022, the Kenya AI Strategy 2025-2028[8] and the Digital Health Act (2023)[9] additionally have made provisions for requirements for regulation of medical devices software prior to market authorization.

1.3 Purpose

The purpose of this guidance document is to promote standardized approach to and consistent expectations on the regulation of Medical Device Software (MDSW) in Kenya

[8] Kenya Ai Strategy 2025-2030
[9] Kenya Digital Health Act (2023)

1.4 Scope

The scope of this document is to define the parameters of regulating MDSW including risk classification requirements, risk management of softwares, Cybersecurity considerations, Artificial intelligence and Machine Learning based medical device software, and the definition of a MDSW.
This document also provides for the definition of a MDSW irrespective of software technology and/or platform (e.g., mobile app, cloud). Software functions that meet the definition of a device may be deployed on mobile platforms, other general-purpose computing platforms, or in the function or control of a hardware device. The policies described in this guidance are independent of the platform on which they might run, are function-specific, and apply across platforms.

Software intended as an accessory to a medical device is not in the scope of this document, unless the software meets the definition of MDSW as defined in this Guideline. An accessory is intended to support, supplement and augment the performance of a parent device.

1.5 Regulatory Context

The Guideline on Submission of Documentation for Registration of Medical Devices, PPB/PER/MDV/GUD/011, outlines the requirements for application submission. However, this new guidance document aims to align with current global practices and advancement for Medical Device Software.

1.6 Specific Considerations

1. Alignment with IMDRF – PPB's regulatory framework aligns with the IMDRF classification principles to ensure harmonization and facilitate international trade and PPB's guideline for registration of medical devices.
2. Risk-Based Approach – the regulatory oversight should be proportional to the risk level of the MDSW. Higher-risk MDSW should undergo more rigorous regulatory scrutiny.

3. Definition of MDSW – clear definitions of SaMD, SiMD, and MDSW are essential to avoid ambiguity and ensure consistent application of regulations.
4. Documentation Requirements – requirements for documentation should be specified based on the classification category. This includes details on intended use, technical specifications, validation, verification, risk management, and post-market surveillance.
5. Ethical Concerns – ethical considerations, such as biases in AI algorithms and data privacy, should be addressed in the regulatory framework.
6. Interoperability – the regulatory framework should promote interoperability with electronic health records and other digital health tools.
7. Safety and effectiveness requirements – the MDSW must meet the safety and effectiveness requirements. For AI/ML, the requirements for safety or effectiveness requirements will be adopted to coincide with current international best practices.

2.0 MEDICAL DEVICE SOFTWARE REGISTRATION

The IEC 62304 standard specifies the process and requirements for the lifecycle of medical device software. The standard applies both to Software as a Medical Device (SaMD) and Software in a Medical Device (SiMD). The framework ensures safety, reliability, and effectiveness of medical device software throughout the medical device development, maintenance and problem resolution phases. Reference should therefore be made to the IEC 62304 standard on the requirements for SaMD and SiMD regulatory requirements.

If a medical device is stand-alone software, guidance for the qualification and classification of the software should be provided with a report of the same. There should be a rationale for why the software is a medical device and for its classification. If applicable, the software should be broken down into modules, some that have a medical purpose and some that do not. The modules with a medical purpose must comply with the requirements of the medical device software registration and carry their own jurisdiction marking. The non-medical device modules are not subject to the requirements for medical device software registration to the extent that they are not claimed otherwise.

Ensure all relevant harmonized and non-harmonized software standards have been considered. Below are the listed harmonized and non-harmonized software standards for consideration. This list of standards is non-exhaustive and other standards may be application in consideration for emerging technologies such as cybersecurity, use of AI. It is the responsibility of the manufacturer to demonstrate application of these standards.

Harmonized Standards

The below listed harmonized standards are for purposes of compliance with specific regulatory requirement

IEC 62304: Medical Device Software – Software Life Cycle Processes	Defines the software development and maintenance life cycle for medical device software, including requirements for risk management, software architecture, and verification/validation.
ISO 14971: Application of Risk Management to Medical Devices	Provides a framework for identifying, evaluating, and controlling risks associated with medical devices, including software-related risks
IEC 60601-1	Includes requirements for software in medical electrical equipment, particularly for safety and performance.
IEC 62366-1	Focuses on the usability engineering process to ensure medical device software is safe and user-friendly

Non- Harmonized Standards

These standards are used to support compliance or improve development processes. They are not officially listed or required for regulatory compliance

ISO/IEC 12207 Systems and Software Engineering – Software Life Cycle Processes	A general standard for software development life cycle processes, not specific to medical devices.
ISO/IEC 27001: Information Security Management	Specifies requirements for establishing, implementing, and maintaining an information security management system, which can apply to medical device software handling sensitive data.
IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems	A general standard for functional safety in programmable systems, not specific to medical devices.
AAMI TIR45: Guidance on the Use of AGILE Practices in the Development of Medical Device Software	Provides guidance on applying Agile methodologies to medical device software development while complying with IEC 62304

Ensure the software systems/ modules/ items have been assigned safety classifications based on standards. Include documentation on the medical device software life-cycle processes implemented (e.g., software design/ development, maintenance/ change management, risk management,

configuration management, problem resolution, verification, and validation processes).

Include software development process documentation (e.g., software development plan, software requirements specification, software architecture, software detailed design, software unit testing procedures/ reports, software integration testing procedures/reports, and software system testing) and maintenance process documentation (e.g., software maintenance plan).

Include software risk assessment documentation (e.g., software hazard analysis, software failure mode and effects analysis, fault tree analysis, traceability).

Note: Some documentation may or may not be required per the standards based on software system/ module/ item risk classification.
Specific information to support the application of software as a medical device requirement will involve provision of information in these sections:

- 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

The following documents listed in Table 1 should be provided as a requisite requirement for registration of MDSW. Appropriate documentation is required if the medical devices are either stand-alone software or rely upon software. Aware of the evolving landscape, the use of stand-alone software is in this reference guidance replaced with MDSW.

Table 1: Document Requirements for registration of a Medical Device Software

No.	Document Required
1	Relevant harmonized and non-harmonized software standards

	- software systems/ modules/ items have been assigned safety classifications based on standards. - Include documentation on the medical device software life-cycle processes implemented - software design/ development, - maintenance/ change management, - risk management, - configuration management, - problem resolution, - verification, and validation processes.
2	Software development process documentation - software development plan, - software requirements specification, - software architecture, - software detailed design, - software unit testing procedures/ reports, - software integration testing procedures/reports, (a software system testing) - maintenance process documentation (e.g., software maintenance plan).
3	software risk assessment documentation - software hazard analysis - software failure mode and effects analysis, - fault tree analysis, - traceability
4	Essential Principles for safety and performance of medical devices
5	Labelling requirements
6	Software versioning and traceability
7	Software verification and validation
8	Clinical evidence
9	Risk management
10	Supporting documents for cybersecurity

2.1 Essential Principles for Safety and Performance

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.

Essential Principles conformity checklists prepared using the essential principal of safety and performance of medical devices and IVDs issued by the IMDRF shall also be submitted for device registration to PPB. The essential design and manufacturing principles that may be relevant to MDSW are listed below against the respective forms of software for reference.

Note that SaMD constitutes a standalone medical device, whereas SiMD refers to software embedded within a device that also incorporates hardware components. Where principles in the table below are listed as applicable to SiMD, they apply to the software component; additional hardware-specific principles may also apply to the overall device incorporating the SiMD.

Table 2: Essential Principles applicable to medical devices and IVDs

Essential design and manufacturing principles	**Software embedded in medical devices (SiMD)**	• **SaMD (including mobile applications and Web-based software)**
General requirements	Yes	Yes
Clinical evaluation	Yes	Yes
Chemical, physical and biological properties	If applicable	Not applicable
Sterility, packaging and microbial contamination	If applicable	Not applicable
Considerations of environment and conditions of use	Yes	Yes
Requirements for active medical devices connected to or equipped with an energy source	Yes	Not applicable
Medical devices that incorporate software or are standalone software or mobile applications	Yes	Yes

Medical devices with a diagnostic or measuring function	Yes	Yes
Labelling and Instructions for use Protection against electrical, mechanical and thermal risks	Yes	If applicable
Protection against radiation	Yes	Not applicable
Protection against the risks posed by medical devices intended for use by lay persons	Yes	Yes
Medical devices incorporating materials of biological origin	If applicable	Not applicable

Essential Principles applicable to medical devices other than IVD medical devices		
Essential design and manufacturing principles	**Software embedded in medical devices (SiMD)**	• **SaMD (including mobile applications and Web-based software)** •
Particular Requirements for Implantable Medical Devices	Yes	Not applicable
Protection against the Risks Posed to the Patient or User by Medical Devices Supplying Energy or Substances	Yes	If applicable
Medical Devices Incorporating a Substance Considered to be a Medicinal Product/Drug	Yes	Not applicable

2.2 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:

- Supplied in physical form or
- Supplied without a physical form
- In both instances, software updates may be provided in physical or without physical form in which case the minimum requirements provided under table 3 apply.

The table below summarises the minimum labelling information to be included for standalone software supplied in either one of the two aforementioned ways.

Table 3: Minimum labelling information to be included for standalone software

Supplied in physical form (i.e., CD/DVD)	**Supplied without any physical and/or digital form- (i.e., downloadable software, web-based software)**
Physical label and Instructions for Use including any special access keys **Essential Device Information;** • Name of device • Software version number • Product owner's information on device labels for identification of the device **For safety and performance information;** • the intended purpose • instructions on proper use	**Essential Device Information**; • Name of device • Software version number • Product owner's information on device labels for identification of the device **For safety and performance information;** • the intended purpose • instructions on proper use • safety information (e.g., contraindications) have to be clearly presented for users' • A screenshot of the software graphical interface (e.g., splash screen) which

• safety information (e.g., contraindications) have to be clearly presented for users' reference • A screenshot of the software graphical interface (e.g., splash screen) which displays the elements for identification, including software version number reference	displays the elements for identification, including software version number reference • In addition, for downloadable software where the downloading and installation is to be done by the end-user, the following information should be presented to the end-user: i. Internet address or web link to allow the end-user to download the software; ii. The software download procedure; and iii. 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.

2.3 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 shall be required during the registration process.

In addition, information on the software version being registered and to be supplied in Kenya 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 submitted. This does not include Software version numbering that is solely for testing or internal use only (e.g., checking in of source code).

2.4 Design Verification & Validation

The MDSW 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 software medical device.

Below are suggested reference documents that can be provided to support the safety and performance of the software medical device:

- The description of the software development process (e.g., according to EN 62304)
- Description of the software design (e.g., according to EN 62304, EN 62366)
- Verification of the software usability according to IEC 62366
- Validation of the software as used in the finished device: e.g., a. summary results of verifications
- Validations and tests performed (in-house or in a simulated or in a real user environment).

Analytical validation of MDSW is 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 and are safely performant in the intended clinical context.[10]

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 are 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.

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 utilization of information among these medical devices or systems have to be in place.

[10] (USFDA, https://www.fda.gov/media/73141/download, 2002)

2.5 Clinical evidence

While software verification and validation ensure 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 to 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 examples:

- 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 MDSW 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 include sensitivity, specificity, positive and negative predictive values.

Where the software is assigned a novel intended purpose or is intended for use in new target populations, manufacturers should generate appropriate association of the software output to the clinical condition/physiological state using clinical evidence.

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, 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.

2.6 Risk Management for Medical Device Software

The ISO 14971 provides for the framework for managing risks associated with medical devices throughout their product lifecycle. The defined process for managing risks, including risk analysis, assessment and control should be considered. Manufacturers should provide risk management as provided for by ISO 14971.

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 software and also the defined intended purpose for the software.

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 MDSW, 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.

2.7 Cybersecurity in Medical Device Software

2.7.1 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 have 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. Continuous monitoring, assessing, mitigating and communicating cybersecurity risks and attacks requires active participation by all stakeholders in the ecosystem.

2.7.2 Principles and Practices for Medical Device Cybersecurity- IMDRF

The principles and practices for Medical Devices cybersecurity provides for general principles and best practices to facilitate international regulatory convergence on medical device cybersecurity.

This document provides an overview of the regulatory requirements in ensuring that the practices for medical devices cybersecurity are considered; such principles emphasize the shared responsibility for cybersecurity with the understanding that patient safety concerns are central. Additionally, the integration of cybersecurity early into the product design provides for the secure software practices and promotes the IEC 62304 'Medical Devices Software Lifecycle' rules.

A Secure product development life cycle encompasses the design, development, deployment and maintenance phases. Implement structured processes for vulnerability and patch management that include continuous monitoring of newly published vulnerabilities (e.g., CVE databases), clearly defined responsibilities for vulnerability disclosure, and seamless patch deployment procedures that ensure no disruption to clinical workflows.

Implement structured processes for vulnerability and patch management that include continuous monitoring of newly published vulnerabilities (e.g., CVE databases), clearly defined responsibilities for vulnerability disclosure, and seamless patch deployment procedures that ensure no disruption to clinical workflows. Transparency and documentations will ensure multi layers of security such that access controls, data encryption and network segmentation for isolating medical devices from hospital IT networks is maintained.

These principles collectively should be considered when considering application for regulation of MDSW.

i. The Kenya Cybersecurity Strategy 2022-2027 and
ii. Kenya Artificial Intelligence Strategy 2025-2030

The cybersecurity framework for medical devices software in Kenya positions cybersecurity and trustworthy AI as core patient-safety, public-health, and national resilience requirements. In alignment with the Kenya National Cybersecurity Strategy (2022–2027) and the Kenya AI Strategy (2025–2030), medical devices software—particularly software incorporating artificial intelligence or machine learning—is recognized as part of Kenya's critical digital health infrastructure. Regulation should therefore require secure-by-design and secure-by-default development practices, risk-based cybersecurity management, and clear governance and accountability throughout the software lifecycle. For AI-enabled medical software, additional regulatory attention is required on data governance, model integrity, algorithmic transparency, and protection against adversarial attacks, model drift, and

unintended bias, consistent with national commitments to ethical, human-centered, and inclusive AI.

Manufacturers, deployers, and operators of medical devices software are expected to safeguard the confidentiality, integrity, availability, and lawful use of health data and AI systems through proportionate technical and organisational controls. This includes requirements for pre-market risk assessment, post-market monitoring, incident detection and reporting, and coordinated response with national cybersecurity and data protection authorities.

In line with the AI Strategy, regulation should also address data sovereignty, third-party and supply-chain risks, validation of AI models used in clinical decision-making, and ongoing performance monitoring to ensure safety, fairness, and reliability over time. Capacity building, local innovation, and collaboration across regulators, developers, healthcare providers, and academia are essential to strengthening Kenya's ability to regulate AI-driven medical software effectively while fostering innovation that supports equitable access to safe, reliable health care.

2.7.3 WHO Cybersecurity Framework Overview

The WHO Cybersecurity Framework provides guidance for countries and healthcare stakeholders to ensure the safe and secure operation of healthcare technologies by embedding cybersecurity across governance, technical controls, and operational processes. It emphasizes strong leadership and accountability for cybersecurity, adoption of risk-based approaches to identify and mitigate threats, protection of devices and software through effective asset and configuration management, and robust access controls to prevent unauthorized use. The framework further highlights the importance of timely incident detection and response, continuous monitoring to address vulnerabilities proactively, and comprehensive data privacy and protection

measures to safeguard patient information in line with international data protection standards.

MDSW regulation shall adopt a risk-based approach consistent with both WHO and national policy frameworks, requiring identification, assessment, and mitigation of cybersecurity and AI-related risks throughout the software lifecycle. Asset management requirements shall ensure visibility, secure configuration, and protection of medical software and associated digital assets, reflecting Kenya's focus on Critical Information Infrastructure Protection and the AI Strategy's emphasis on trustworthy, reliable systems. Strong access control mechanisms shall be mandated to prevent unauthorized use or manipulation of medical software, while safeguarding clinical integrity and patient safety.

In alignment with the Kenya Cybersecurity Strategy, MDSW regulation shall require robust incident detection, reporting, and response mechanisms, including coordination with national cybersecurity authorities for incidents that may affect service continuity or public safety. Continuous monitoring obligations shall support early identification of vulnerabilities, cybersecurity threats, and AI performance degradation such as model drift. Consistent with the Kenya AI Strategy, regulation shall also address data governance, algorithmic integrity, transparency, and human oversight, ensuring that AI-enabled medical software operates ethically, lawfully, and safely. Collectively, this alignment future-proofs Kenya's MDSW regulatory framework by embedding global best practices while supporting innovation, local capacity building, and trusted deployment of digital and AI-driven medical technologies.

2.7.4 Cybersecurity Considerations in the regulatory system

When developing a software medical device, a cybersecurity plan should be devised to include the following considerations and not limited to:

(i) 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	● User authentication - ensure access to device only to be granted to users after they have been authenticated. e.g., using of passwords/encryption key/privilege roles ● Carry out authorization checks during execution of commands, software updates or external connection, to request for use authentication ● User access controls -employing a layered authorization model by differentiating privileges based on user roles or device functions' e.g systems administrator/ caregiver
Detecting potential cybersecurity risks	● Continuous monitoring- ensure there are routine security or antivirus scans to detect any security compromise. ● Devices should also have a security event logging system to trace any attacks.
Responding to cybersecurity incidents	● Impact mitigation - there should be a notification system to alert users of detected attacks. ● In build secure configurations like anti-malware/ firewall should also be in place to limit impact of attack.
Recovering from Cybersecurity incidents	● Device functional recovery - a system should be in place that deploys patches/ updates efficiently. ● Authenticated privileged users should also be able to recover device configuration effectively.

(ii) Customer Security Documentation – besides supplying the end users with the instructions for use (IFU) on the appropriate usage of the MDSW, manufacturers should also consider providing customer

security documentation to communicate the relevant security information to mitigate cybersecurity risks when operating the MDSW 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 MDSW 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 networks, 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 MDSW 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 MDSW 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.

(iii) 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:

- identify all possible cybersecurity hazards,
- assess the associated risks,
- implement mitigations or controls to reduce risks to acceptable level,
- 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 processes should be conducted in parallel with safety risk management.
- The overall patient safety should be considered when introducing security measures to 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 an 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, the 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.

(iv) 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 the 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.

(v) 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 MDSW 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. Information Sharing and Analysis Organization (ISAOs), Information Sharing and Analysis Centers (ISACs) etc.

(vi) Patient confidentiality, privacy and other regulations - medical device cybersecurity incidents can affect patient safety and privacy. There are

increasing reports of breaches of data privacy. MDSW developers, implementers and users should always be vigilant in handling confidential patient data. All should comply with the Data Protection Act No 24 of 2019 and Kenya's digital health Act No.15 of 2023.

2.8 Artificial Intelligence (AI) Enabled Medical Devices

One of the greatest potential benefits of AI enabled medical devices resides in the ability to improve model performance through iterative modifications, including by learning from real-world data.[11]

To promote safe, effective and high-quality medical devices that use AI and ML, the adoption of the ten (10) guiding principles that can inform the development of Good Machine Learning Practice (GMLP) is important for consideration.

These ten (10) guiding principles are intended to lay the foundation for developing Good Machine Learning Practice that addresses the unique nature of these products. They will also help cultivate future growth in this rapidly progressing field.

The ten (10) guiding principles identify areas where the International Medical Device Regulators Forum (IMDRF), international standards organizations, and other collaborative bodies could work to advance GMLP. Areas of collaboration include research, creating educational tools and resources, international harmonization, and consensus standards, which may help inform regulatory policies and regulatory guidelines.

Guiding Principles

1. Multi-disciplinary expertise is leveraged throughout the total product life cycle
2. Good software engineering and security practices are implemented
3. Clinical study participants and data sets are representative of the intended patient population
4. Training data sets are independent of test sets

[11] (USFDA, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial-intelligence, 2025)

5. Selected reference data sets are based upon best available methods
6. Model design is tailored to the available data and reflects the intended use of the device
7. Focus is placed on the performance of the human-AI team
8. Testing demonstrates device performance during clinically relevant conditions
9. Users are provided clear, essential information
10. Deployed models are monitored for performance and re-training risks are managed

2.8.1 Regulatory Requirements for AI Enabled Medical Devices

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

All activities related to the design, development, training, validation, retraining and deployment of AI based MDs should be performed and managed under an ISO 13485 based quality management system (QMS).[12]

Additionally, specific data that should be submitted for registration of AI based MDs should include the following:

Requirements	**Description**
I. Dataset	
a) 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 based MDs 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

[12] (Health Sciences Authority, Singapore:Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach, 2022)

	to be provided for the pre-processing steps applied to the input data.
b) 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.
II. AI Model	
AI model selection	• A description on the machine learning model (e.g., convolutional neural network) used in the AI based MDs, including any base model (e.g. Inception V3 model), should be provided. • Appropriateness of the model for the AI based MDs 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.
III. Performance and Clinical Evaluation	
a) Test protocol and report for verification and validation of the AI based MDs, including the acceptance limits and information on the anomalies identified	• Based on the performance specification of the AI based MDs, the test protocol and test report should be provided. • Information on control measures to detect extremes/outliers should be provided. • Any limitation of the AI based MDs and the operating system must be clearly evaluated and also communicated as appropriate to the user in the product labelling or instruction manual.
b) Performance of the AI based MDs (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.
c) Clinical Association between the AI based MDs output and clinical conditions(s) must be presented	• Presence of a valid clinical association between the AI based MDs output and its targeted clinical condition should be presented.
IV. Deployment	
a) 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.

b) Interval for training data update cycle (e.g., in months or years)	• In cases where data is collected after the deployment of the AI Enabled MDs (fixed-version) and these datasets are used to re-train the subsequent models of the AI based MDs, 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 PPB in accordance with applicable change notification guidelines. Similar to other software, a Change Notification will be required for changes to registered AI Enabled MDs. This includes any changes to the performance specifications, input data types, device workflow, degree of human intervention, choice of AI model, etc.
c) Software version to be supplied in Kenya and the procedure or plan implemented to trace the software version for subsequent iterations	• For the purpose of post-market traceability, the exact AI based MDs version to be supplied in Kenya and explanation on how the version numbers are designated and traced should be provided.

2.8.2 AI based MDs with Continuous Learning Capabilities

AI based MDs with continuous learning capabilities have the ability to change their 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 based MDs post-learning. This is important to ensure that the learning does not compromise the defined specifications or output of the AI based MDs. As the AI based MDs with continuous learning capabilities can automatically change their 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 based MDs does not deteriorate over time.

For continuous learning AI based MDs, complete information on the learning process including the process controls, verification and ongoing model monitoring measures shall be clearly presented for review in the application for registration of the AI based MDs.

The following information should be submitted:

i. Description of the process of continuous learning of the AI based MDs during deployment.
ii. 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 a process to detect and roll-back to the previous algorithm version which includes criteria by which the system is measured against (baseline).
iii. During deployment, the AI based MDs will learn from real world data. The source, data type collected, data pre-processing steps and parameter extracted should be defined to ensure there are no biases in the process. The inclusion and exclusion criteria should be listed and this should be identical to the attributes of the original training dataset
iv. Process to ensure data integrity, reliability and validity of the new data set used for learning
v. Software version control mechanisms should be designed and implemented to accommodate systems that may undergo frequent updates, including continuously learning systems. Where feasible, this should include the ability to track, document, and distinguish versions across deployment sites—whether updates are applied globally or adapted locally. In addition, systems should be designed to enable ongoing performance monitoring and, where necessary, support rollback or reversion to a prior validated state, recognizing that such capabilities are not inherent to all systems and must be planned for during system design and deployment. If the AI based MDs are deployed in a decentralized environment, there should be robust

processes in place to address the risks involved in such a decentralized model. Other process controls for consideration include maintaining traceability, performance monitoring and change management.

vi. Process to ensure traceability between real world data for training, learning process, software version number and the AI based MDs Output during clinical use. When there are inaccurate results during deployment due to biased real-world data, manufacturers must be able to trace back to the specific data and remove such data from the AI model and retrain the models as necessary.

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

2.8.3 Post-market Monitoring of AI based MDs

Once AI based MDs are deployed in the real-world environment, active monitoring, review and tuning are necessary. 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 based MDs deployed in clinical settings. Such monitoring could also be in the form of autonomous monitoring embedded in the system. A robust surveillance model to ensure that the AI based MDs 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.

For all registered AI based MDs locally, companies are required to monitor the real-world performance post deployment and submit periodic post-market reports to the Board through https://pv.pharmacyboardkenya.org .This allows close monitoring and detection of any failure of these AI based MDs by PPB and where necessary enables timely intervention post deployment of the AI based MDs.

The applicant shall submit to PPB a commitment to provide periodic post-market reports and further ensure the same reports are filed annually during the life cycle of the MDSW and AI based MDs.

2.9 MDSW Categorization Criteria

This section provides an approach to categorize MDSW based on the factors identified in the definition statement.

2.9.1 Categories Based on Risk and Impact

The following are the principles to guide the risk – impact-based categorization of MDSW

1. Intended Use – the specific medical purpose for which the MDSW is intended plays a significant role. This includes whether the software is used for diagnosis, treatment, monitoring, or prevention of diseases.
2. Significance of information provided by MDSW – the impact of the information provided by the MDSW on clinical management and patient outcomes is a critical factor. If the information is used to drive critical decisions or interventions, the risk level is higher.

   Note: Many jurisdictions use the rules-based system that relies on classification rules within their regulations. Those rules ultimately determine the classification of a device, and ultimately reference is made to the GHTF/SG1/N15 (Principles of Medical Devices Classification). Further the IMDRF Guidance documents N12, N81 Provide additional useful guidance on jurisdictions using the risk classification. However, it is the wording of our classification rules (reference in the guideline for registration of medical devices in Kenya) that ultimately dictates the risk classification. Please note that not all jurisdictions use this rules-based approach for their classification.
3. State of the healthcare situation or condition – the severity of the condition that the MDSW is intended to address influences its classification. MDSW intended for critical conditions or situations where delayed or inaccurate information could lead to significant harm will be classified higher.

2.9.2 IMDRF Risk Categorization

The IMDRF risk-based categorization framework provides for four (4) categories based on the combination of the significance of the information, intended use and the state of healthcare as follows:

Table 4: Risk-based categorization of SaMD

The resulting SaMD category and the associated regulatory consideration is provided as follows:

State of Healthcare Condition	**Significance of Information Provided by SaMD**		
	Treat or diagnose	Drive clinical management	Inform clinical management
Critical	IV	III	II
Serious	III	II	I
Non-serious	II	I	I

Risk Category	**Description**
Category I	• **Low Risk:** SaMD that provides information for general wellness, lifestyle management, or administrative purposes. The information provided has minimal impact on clinical management. • **Regulatory Consideration:** Minimal regulatory oversight may be required. General Good Software Development Practices and Quality Management Systems may suffice.
Category II	• **Medium Risk:** SaMD that provides information to inform clinical management decisions. The information has a moderate impact on patient outcomes. • **Regulatory Consideration:** Moderate regulatory oversight is necessary. Requirements may include documentation of validation, verification, and risk management processes in addition to the requirements for Category I.

Category III	• **High Risk:** SaMD that drives or treats critical clinical conditions or provides information that directly impacts critical patient management decisions. Errors or inaccuracies can lead to significant harm. • **Regulatory Consideration:** Stringent regulatory oversight is required. This includes pre-market review, clinical evaluation, post-market surveillance, and adherence to specific standards in addition to the requirements for Category II.
Category IV	• **Very High Risk:** SaMD that is intended to treat or diagnose critical conditions and where inaccurate information or malfunctions can lead to death or serious irreversible harm. • **Regulatory Consideration:** Very stringent regulatory oversight, including rigorous pre-market approval, extensive clinical trials, and ongoing post-market monitoring in addition to the requirements for Category III.

2.10 Submission of Applications for MDSW

a) To access the Medical Devices Software application portal, the applicant MUST have an active online account with PPB which is accessed by logging into PPB Pharmacy and Poisons Board Regulatory Information Management System (PRIMS) Portal (https://prims.pharmacyboardkenya.org).

b) The applicant shall select the Medical Devices Software application option.

c) The applicant shall dully fill an Application Form (***refer to Annex II***), Letter of Authorization (***refer to Annex V***) and upload the requisite documentation as provided in the guideline.

d) The application shall be submitted through PPB PRIMS online portal. (https://prims.pharmacyboardkenya.org)

e) Upon submission of a completed application an invoice will be generated in line with the MDSW category.

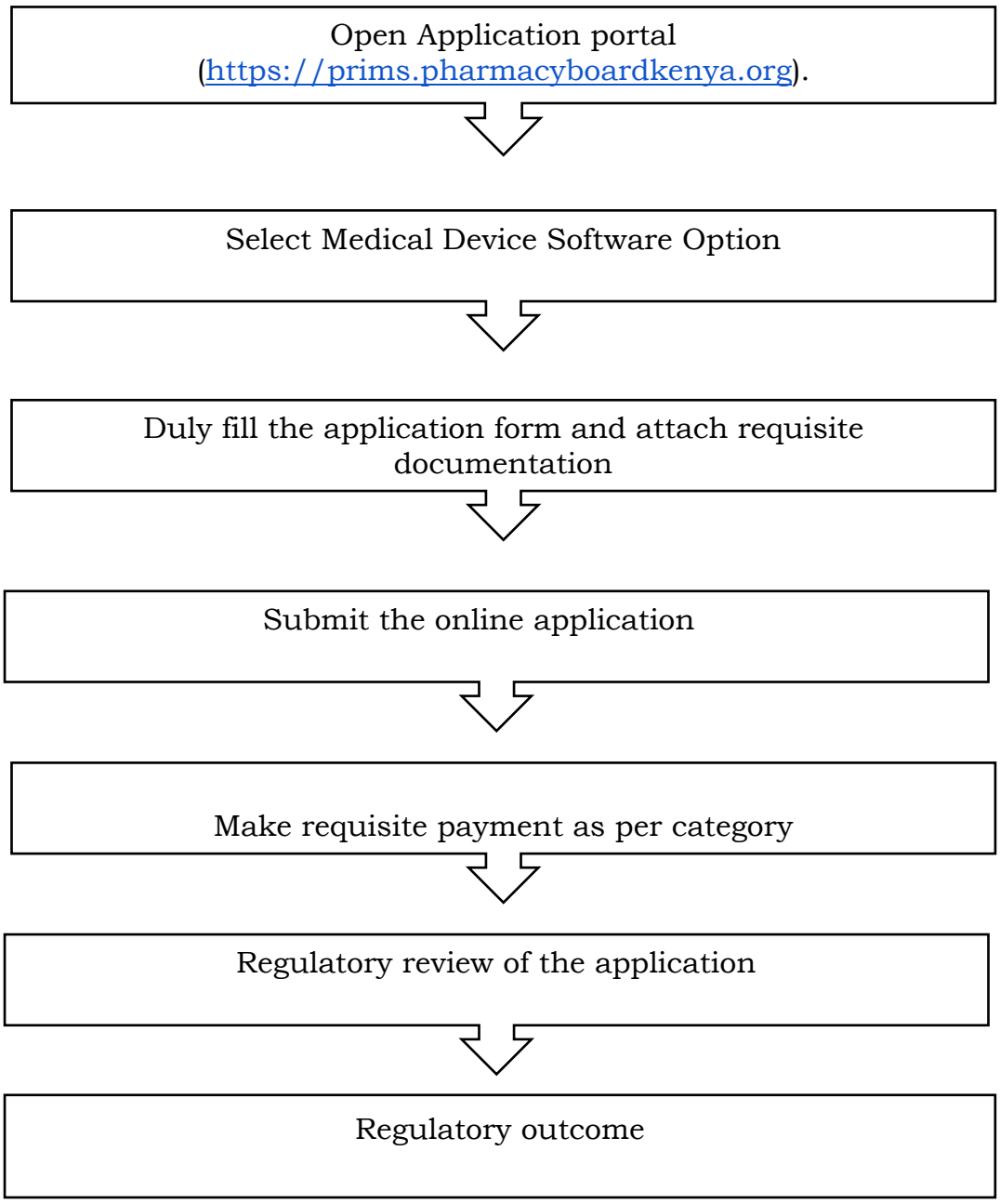
f) The applicant shall pay requisite fee as per the invoice generated.

g) A unique MDSW reference number is automatically assigned for the application and it will be used in all subsequent correspondences relating to the application throughout the application process and MDSW lifecycle.

h) Review of the application by PPB will be based on information submitted by the applicant.

i) Regulatory Outcomes shall be communicated to the applicant.

MDSW Application Process Flow



2.11 Changes to MDSW and Re-evaluation of Category

A medical device software 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 Board shall employ 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.

Significant changes may include, but not limited to, any of the following:

i. The manufacturing process, facility or equipment;
ii. The manufacturing quality control procedures, including the methods, tests or procedures used to control the quality, purity, safety and sterility of the device or of the materials used in its manufacture;
iii. The design of the device, including its performance characteristics, principles of operation and specifications of materials, energy source, software or accessories.
iv. Any addition or deletion of a contraindication for the device, and any change to the period used to establish its expiry date.
v. For AI enabled MDs if a new set of data collected changes the original specification and performance of the device, a Change Notification should be submitted to The Board

As such, non-significant software changes are required to be notified to the Board Such Notification changes may be bundled and notified in one change notification application. Alternatively, such changes could be submitted

together with the next Review/Technical change of the registered software (whichever comes first). While bundling Notification changes, any such change shall be submitted to the board from the point of first implementation, to the extent applicable in Kenya. Prior to implementation of notification changes in Kenya, companies shall maintain relevant inventory records on file to ensure traceability of the changes as part of their QMS requirements.

Similar to other registered medical devices, a Change Notification will be required for any changes made to a registered AI enabled medical device. If there are changes to the MDSW that affect its definition statement, the categorization should be revised. This ensures that the MDSW is appropriately classified based on intended use. Some changes that will **NOT** qualify for Change Notification and shall require the submission of a **NEW** application. Such changes include:

i. Change to the intended use of a registered MDSW.
ii. Change to the risk categorization of a registered MDSW.
iii. Change to the medicinal substance in a device that incorporates a medicinal product in an ancillary role.

Further guidance is provided for in the Guidelines On Change Notification/Variation Of Registered Medical Devices Including In-Vitro Diagnostics

The changes referenced below refer to additional changes for MDSW.

Table 5: Requirement for change in Medical Device Software

Type of change	**Description**	**Documents required**
1. **Significant Changes**	a) Change in relevant harmonized and non-harmonized software standards.	Provide reports/supporting documents on: • Software design/ development • maintenance/change management. • Risk management report. • Configuration management, • Problem resolution.

		• Verification and validation processes.
	b) Change in intended use/purpose.	• Clinical evidence reports. • Updated IFU.
	c) Change in software development process.	• Software validation reports. • Detailed summary of software changes. • software development plan, • software requirements specification, • software architecture, • software detailed design, • software unit testing procedures/ reports, • software integration testing procedures/reports, (a software system testing) • Maintenance process documentation (e.g., software maintenance plan).
	d) Change in Instruction for use e.g Modification of device design, materials or manufacturing process	• Provide the medical device file section of MDSW showing the changes to the IFU • Justification for the revision.
	e) Change in Labelling.	• Description of the warning, precaution or contraindication. • Justification for the revision. • Useability test reports (If applicable).
	f) Changes in software versioning, and traceability	• Software Requirement Specifications (SRS). • Traceability matrix. • Revision history. • Provide evidence on change of version and build number convention. • Change management records.

		• Unique device Identifier (UDI)/Product Identifier (PI), where applicable.
	g) Changes in Software verification, validation and security	• Verification and validation report. • Supporting document for cybersecurity
2. Non-significant Changes	a) Change in manufacturing site address. b) Updated list of configurations of MDSW. c) Declaration of conformity. d) Change in colour of labelling. List of non-significant changes is non exhaustive and the examples provided are a guide.	Provide documentation to support the change**.**

Applications for changes for a registered MDSW shall be submitted as per **Annex III** for non-significant changes and **Annex IV** for significant changes.

2.12 Fees

The independent review of Medical Devices Software (MDSW) will be implemented through the portal www.Pharmacyboardkenya.org

The proposed fee structure:

Risk Classification	**Foreign Manufacturer Fee Structure in USD**	**Local Manufacturer in USD**
Administrative fee	300	100
Category I&II	500	250
Category III	2,000	1,000
Category IV	2,500	1,250

Under the Health Products and Technologies Act, all HPTs shall be issued with a certificate of registration valid for a period of five (5) years.

3.0 REVISION HISTORY

Revision No:	Date	Prepared by	Section(s) revised	Description of change
0		QAO	All Sections	Initial issue of the guideline

4.0 REFERENCES

1. European Commission-Medical Device Coordination Group. (2019, October 1). *Guidance on qualification and classification of software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR*. https://health.ec.europa.eu/system/files/2020-09/md_mdcg_2019_11_guidance_qualification_classification_software_en_0.pdf
2. GHTF-Label and Instructions for Use for Medical Devices. (2011, September 16). *Label and instructions for use for medical devices*. https://www.imdrf.org/sites/default/files/docs/ghtf/archived/sg1/technical-docs/ghtf-sg1-n70-2011-label-instruction-use-medical-devices-110916.pdf
3. Health Canada. (2019, December 18). *Software as a medical device (SaMD): Definition and classification*. https://www.canada.ca/content/dam/hc-sc/documents/services/drugs-health-products/medical-devices/application-information/guidance-documents/software-medical-device-guidance-document/software-medical-device-guidance-document.pdf
4. Health Sciences Authority, Singapore. (2022, April 21). *Regulatory guidelines for software medical devices – A life cycle approach*. https://www.hsa.gov.sg/docs/default-source/hprg-mdb/guidance-documents-for-medical-devices/regulatory-guidelines-for-software-medical-devices---a-life-cycle-approach_r2-(2022-apr)-pub.pdf
5. IMDRF Software as a Medical Device (SaMD) Working Group. (2013, December 9). *Software as a medical device (SaMD): Key definitions*. https://www.imdrf.org/sites/default/files/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf
6. IMDRF Software as a Medical Device (SaMD) Working Group. (2014, September 18). *Software as a medical device: Possible framework for risk categorization and corresponding considerations*. https://www.imdrf.org/documents/software-medical-device-

possible-framework-risk-categorization-and-corresponding-considerations

7. IMDRF Software as a Medical Device Working Group. (2025, January 30). *Characterization considerations for medical device software and software-specific risk*. https://www.imdrf.org/documents/software-medical-device-possible-framework-risk-categorization-and-corresponding-considerations
8. U.S. Food and Drug Administration. (2021, October 21). *Good machine learning practice for medical device development: Guiding principles*. https://www.imdrf.org/documents/good-machine-learning-practice-medical-device-development-guiding-principles
9. U.S. Food and Drug Administration. (2022, September 29). *Digital health terms*. https://www.fda.gov/medical-devices/digital-health-center-excellence/digital-health-terms
10. U.S. Food and Drug Administration. (2024, December 4). *Marketing submission recommendations for a predetermined change control plan for artificial intelligence-enabled device software functions*. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/marketing-submission-recommendations-predetermined-change-control-plan-artificial-intelligence
11. U.S. Government-Office of the President Federal Register. (2023, October 30). *Safe, secure, and trustworthy development and use of artificial intelligence*.

5.0 LIST OF CONTRIBUTORS/REVIEWERS

No.	Name	Department
	Dr Ahmed Mohamed	Chief Executive Officer
	Dr Ali Arale	Ag.Director Health Products and Technologies and Chief Principal Regulatory Officer Department of Product Evaluation and Registration, PPB
	Dr Kariuki Gachoki	Deputy Director, Department of Product Evaluation and Registration, PPB
	Dr Paulyne Wairimu	Senior Principal regulatory officer, Medical Devices and In-Vitro Diagnostics
	Erick Kitangala	Principal Regulatory Officer, Department of Product Evaluation and Registration, PPB
	Alex Mutai	Principal Regulatory Officer, Department of Product Evaluation and Registration, PPB
	Solomon Koech	Principal Regulatory Officer, Department of Product Evaluation and Registration, PPB

LIST OF REVIEWERS

List of Reviewers	
Dr. Johnathan Meriakol	Dr Vallarie Khamira
Dr Felistas Chepwogen	Dr Gitobu Kireran
Dr. Edwin Burugu	Dr Purity Mutinda
Dr Paulyne Wairimu	Dr Emmanuel Munguti
Dr Eugene Odame	Dr Kauthar Bajaber
Dr Solomon Koech	Dr Beatrice Cheruiyot
Mr Alex Mutai	Dr Anushree Patel
Mr Bryhan Kariuki	Dr Shellan Omondi
Mr Henry Chweya	Dr. Anne Tibin
Dr Brayhan Kariuki	Dr. Francis Letipila
Mr Amos Kiprono	Ms Maureen Njiru

6.0 ANNEXURES

Annex I: Examples of software that do not meet the requirements for regulation.

Statement of a software		**Examples**
Software that provides patients with simple tools to organize and track their health information.	These apps do not provide alerts or recommendations to alter or change a previously prescribed treatment or therapy.	Examples include: apps that provide simple tools for patients with specific conditions or chronic diseases (e.g., obesity, anorexia, arthritis, diabetes, heart disease) to log, track, or trend their events or measurements (e.g., blood pressure measurements, drug intake times, diet, daily routine or emotional state) and share this information with their health care provider as part of a management plan.
Software that meets the definition of Medical Device Data Systems (MDDS)	These are software that are intended to transfer, store, convert format, and display medical device data, without controlling or altering the functions or parameters of any connected medical device.	This software includes those that are used as a secondary display to a regulated medical device when these applications are not intended to provide primary diagnosis, treatment decisions, or to be used in connection with active patient monitoring e.g., Electronic Health Record Interphases, Software that transfers patient data (vital signs, laboratory results) without altering the data.
Chat-based triage software intended to guide users to the most appropriate form of help based on their medical symptoms.	The chat-based triage software outcomes are intended to indicate to a user the next best step to take when seeking further health care, and to provide safe and	Triage advice outcomes include self-care, pharmacy, primary care, dental, ophthalmic, sexual health and emergent care advice outcomes.

Statement of a software		**Examples**
	appropriate clinician-vetted advice where appropriate.	
Software intended to be used as an annotation tool for the production of diagnostic and prognostic reports of clinical electroencephalogram (EEG) studies, based on a user's traditional visual interpretation of EEG.	It is intended to standardize and structure reporting of clinical EEG according to an international academic standard.	The software is also intended to reduce the workload of the reporting doctor by automatically importing minimal pieces of information from an external EEG system.
Software that incorporates a risk calculator based on well-established, publicly available models to generate a score for obese individuals at risk of developing heart disease.	This includes software applications intended to provide a convenient way for clinicians to perform various simple medical calculations routinely used in clinical practice.	This software is tailored for clinical use, but retains functionality that is similar to simple general-purpose tools such as paper charts, spread sheets, timers or generic mathematical calculators.
Software that provides supplemental care by coaching or educating patients to help them manage their health.	This includes software that complements professional clinical care by facilitating behavioural change or coaching patients with specific diseases or conditions in their daily environment.	Examples include software that coaches patients with conditions such as cardiovascular disease, hypertension, diabetes or obesity, and promotes strategies for maintaining a healthy weight, getting optimal nutrition, exercising and staying fit, managing salt intake, or adhering to pre-determined medication dosing schedules by simple prompting.
Software that calculates drug dosing based on the information provided on a drug product label.	The user manually inputs the necessary parameters (e.g., age, gender, weight) to determine the appropriate dose.	The user is able to independently review the calculation.

Statement of a software		**Examples**
Software that converts paper-based mental health assessments to an electronic format	These paper-based assessments are readily available to the medical community and are routinely used in clinical practice. The type of information must be from authoritative medical sources, as recognized by the field or discipline that is the subject of the assessment, and must be cited in the software.	The results can be independently reviewed by a healthcare professional.
Clinical-Coding Information System Application Software that receives, collects, stores, manages, assists in analysis of, displays, outputs and distributes data	Healthcare facilities use the software to support the administrative and clinical activities associated with the electronic registration of patient diagnoses and procedures (used within or between facilities).	This software is not considered a medical device when used to triage patients who arrive at an emergency department.
Software that serves as a medical image storage device by providing electronic storage and retrieval functions for medical devices or software that serves as a medical image communication device by providing electronic transfer of medical image data between medical devices.[13]		

[13] https://www.canada.ca/en/health-canada/services/drugs-health-products/medical-devices/application-information/guidance-documents/software-medical-device-guidance/examples.html#a4.3

Annex II: Template for Application of Medical Device Software (MDSW)

Application Form	
Applicant Details	
Name of Applicant (Physical Address and Contact Details)	
MAH (Physical Address and Contact Details)	
LAR: Local Authorized Representative (Physical Address and Contact Details)	
Country of Origin	
Local/Foreign	Should populate invoice amount based on this
MDSW Details	
Software Trade Name	
Common Name	
Software Version Number	
UDI-Unique Device Identification	
Software type	
Intended use	
Medical Purpose	
Description of the software	
MDSW Type	SaMD SiMD
MDSW categorization	Category I, Category II, Category III, Category IV
Software Lifecycle	
Mode of supply	physical and non-physical forms
Registration Status in Other Countries	
Software Operation Environment (Standalone software only)	

Documentation Required	
S/No	**Required Documentation**
1.	Relevant harmonized and non-harmonized software standards
2.	System and software design
3.	software verification & validation
4.	Essential Principles Checklist
5.	Risk Management File
6.	Post Market Surveillance Commitment & reporting
7.	Cybersecurity Plan
8.	Clinical evidence and Clinical Studies
9.	Device Labelling & Instructions for Use
10.	Biocompatibility studies *(if applicable)*
11.	Quality Management System

Declaration

I confirm that I have neither amended the wording in this application, nor otherwise altered the documentation material in any manner, apart from filling in the blanks. I declare that the information provided in this application is accurate and correct and the device conforms to all the applicable requirements stipulated above.

The Applicant:

Name: ……..

Position: ……

Signature: ……

Date: ……

Annex III: Variation Template Non-Significant change

Type of Change (Non-significant)	
Current Status	Proposed Change
Justification of Change	

Annex IV: Variation Template Significant change

Type of Change (Significant)	
Current Status	Proposed Change
Justification of Change	
Required Documentation as per Table 5**;** Requirement for change in Medical Device Software	

Annex V: Letter of Authorization Template

[To be printed on Company Letterhead of Product Owner]

Medical Device Department

Pharmacy and Poisons Board Lenana Road Offices

P.O Box 27663-00508

Nairobi, Kenya.

[Date]

Dear Sir/Madam,

Subject: Letter of Authorization for *[name of Registrant (Company Name)]*

We, *[name of Product Owner]*, as the Product Owner, hereby authorise *[name of Registrant (Company Name)]*, as the Registrant to prepare and submit applications for the evaluation and registration of Medical Devices Software to the Pharmacy and Poisons Board on our behalf.

This authorisation shall apply to the following Medical Device Software(s):

[List containing product names of medical devices]

We also authorise *[name of Registrant (Company Name)]* to make declarations and to submit documents on our behalf, regarding the above Medical Device Software(s), in support of this application. These declarations and submissions are made pursuant to the requirements of the Health Act 2017, which includes the Health Products and Technologies and any other applicable laws that may also be in force.

This authorisation shall remain in effect until our notification to the Pharmacy and Poisons Board in writing (either by postal mail or facsimile transmission) that the authorisation is revoked.

We undertake to provide post-market support and assistance to the Registrant as may be required in relation to any matter involving the

above Medical Device Software(s).

We acknowledge that any non-compliance with any registration condition issued by the Pharmacy and Poisons Board in relation to medical devices registered in Kenya may result in the suspension or cancellation of the Medical Device Software(s) registration.

We give exclusive rights to the LAR for importation, registration and distribution of our product in Kenya we give exclusive rights for the importation, registration and distribution has been given to the LAR

We agree to assist the Pharmacy and Poisons Board with any request for information on the above Medical Device Software(s).

Yours Sincerely,
[Signature]
[Full Name and Title of Senior Company Official] [Company stamp

Pharmacy and Poisons Board
P. O. Box 27663- 00506 Lenana Road Opposite Russian Embassy Nairobi,
Tel: +254 709 770 100
Website: webmaster@ppb.go.ke
Email: info@ppb.go.ke