TR-007:2023(E)

Medical Device Administrative Control System (MDACS)

Software Medical Devices and Cybersecurity

Technical Reference: TR-007

中華人民共和國
香港特別行政區政府衞生署

Department of Health
The Government of the Hong Kong Special Administrative Region
The People’s Republic of China

Revision History

Edition Number	Date of Revision	Summary of Revision	Reference Number
0	29 December 2023	• First issue of TR-007	TR-007:2023(E)

Table of Contents

1. Introduction

1.1 Background

1.1.1 Under the existing framework, the Medical Device Administrative Control System (MDACS) addresses public health risks of software for both software embedded in a medical device (MD), i.e. Software in a Medical Device (SiMD) and standalone software, i.e. Software as a Medical Device (SaMD) in the Essential Principles of Safety and Performance of Medical Devices. Due to the advancement of technology and the global trend of MD control, more up-to-date elaboration is required on the control for SiMD and SaMD, especially the latter, so as to strike a balance between patient/consumer protection and facilitating innovation.

1.1.2 Digitisation and wireless connection of MDs improve the device performance and the efficiency of healthcare services. On the other hand, it may pose a risk of revealing the vulnerability of the system through the use of network. Cybersecurity threats has been a critical issue for MD manufacturer's consideration during software development, so that patient data and clinical services could be protected from network vulnerable attack.

1.1.3 This document aims to provide:

- an overview of software developed for medical purpose;
- the concept of classification of software MDs under the framework of MDACS classification principle for these MDs; and
- the basic requirements on cybersecurity of MD under MDACS.

2. Scope

2.1 This document focuses on the overview and definition of software MDs.

2.2 This document aims to provide a definition for:

2.2.1 SiMD when software is embedded in an MD, and

2.2.2 SaMD when standalone software is considered to be an MD.

2.3 This document also provides guidance for its listing including classification and cybersecurity requirements under MDACS.

3. Definitions and Abbreviations

3.1 **"Software as a Medical Device" (SaMD)** is defined as software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device.

NOTES:

- SaMD is an MD and includes General Medical Device (GMD) and In Vitro Diagnostic Medical Device (IVDMD).
- SaMD is capable of running on general purpose (non-medical purpose) computing platforms including hardware and software resources (e.g. operating system, processing hardware, storage, software libraries, displays, input devices, programming languages, etc.).
- "without being part of" means software not necessary for a hardware MD to achieve its intended medical purpose(s).
- Software does not meet the definition of SaMD if its intended purpose is to drive a hardware MD.
- SaMD may be used in combination (e.g. as a module) with other products including MDs.
- SaMD may be interfaced with other MDs, including hardware MDs and other SaMD software, as well as general purpose software.
- Mobile apps that meet the definition above are considered SaMD.
- SaMD may also:
    - provide means and suggestions for mitigation of a disease; or
    - provide information for determining compatibility, detecting, diagnosing, monitoring or treating physiological conditions, states of health, illnesses or

congenital deformities; or

- aid to diagnosis, screening, monitoring, determination of predisposition, prognosis, prediction, determination of physiological status.

3.2 **“Software in a Medical Device” (SiMD)** is defined as software intended to be used for one or more medical purposes that perform these purposes by controlling and operating a hardware medical device or operating in a medical computing platform.

3.3 **Intended use/purpose** see Clause 2.24 of GN-00.

3.4 **Medical Purpose**

The following two terms as defined in Guidance Notes GN-00 identify medical purpose applicable to SiMD and SaMD:

3.4.1 **Medical Device** see Clause 2.36 of GN-00.

3.4.2 **In Vitro Diagnostic Medical Device** see Clause 2.27 of GN-00.

3.5 Please refer to Guidance Notes GN-00 (Guidance Notes for Definitions and Abbreviations for Medical Device Administrative Control System) for the definitions and abbreviations of the terms that appear in this document.

4. Software medical devices

4.1 Software for medical purpose include both SiMD and SaMD.

4.1.1 SiMD is defined as software intended to be used for one or more medical purposes that perform these purposes by controlling and operating a hardware medical device or operating in a medical computing platform. For example:

- Software that is intended to be used to operate a clinical chemistry analyser.

- Software embedded in electrocardiograph (ECG) machine intended to control the device to measure ECG signal from patient and print the result.

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

4.1.3 SaMD may also:

- provide means and suggestions for mitigation of a disease; or
- provide information for determining compatibility, detecting, diagnosing, monitoring or treating physiological conditions, states of health, illnesses or congenital deformities; or
- aid to diagnosis, screening, monitoring, determination of predisposition, prognosis, prediction, determination of physiological status.

4.1.4 For example:

- Software that analyses heart rate data intended for a clinician as an aid in diagnosis of arrhythmia.
- Software that interpolates data to provide three-dimensional reconstruction of patient's computer tomography scan image, to aid in the placement of catheters by visualisation of the interior of the bronchial tree in lung tissue and placement of markers to guide radiosurgery and thoracic surgery.
- Software that uses the microphone of a smart phone to detect interrupted breathing during sleep and sounds a tone to rouse the sleeper.
- Software that is intended to provide sound therapy to treat, mitigate or reduce effect of tinnitus for which minor therapeutic intervention is useful.

5. Listing of software medical devices under MDACS

5.1 Software for medical purpose is also considered as an MD under MDACS.

5.2 Classification of software MDs shall follow the risk-based classification principle in accordance with Technical Reference TR-003 (Classification of General Medical Devices) and TR-006 (Classification of In Vitro Diagnostic Medical Devices (IVDMDs)).

5.2.1 SiMD usually incorporates with a hardware MD as part of the component / accessories. It should be classified according to the intended use of the combination. Applicants are advised to list this software with the associated hardware MD. In case the applicants wish to list SiMD independently, they shall provide sufficient justifications to demonstrate the necessity of the individual listing of the SiMD during submission of listing application and clearly state whether the corresponding hardware MD(s) is/are going to be listed under MDACS. Such application shall be subjected to Medical Device Division's (MDD) agreement.

5.2.2 SaMD usually operates alone and is not necessary to work with hardware MD. In general, SaMD should be listed independently. It is classified in its own right using the classification rules in TR-003 and TR-006.

5.3 Applicable Classification Rules

5.3.1 Software MDs are deemed to be active device under MDACS classification.

5.3.2 For SiMD, the software is embedded/installed in a hardware MD to perform a specific medical purpose and should generally be listed with the hardware MD. Should individual listing/classification be needed:

- Rule 11 may also be applicable when the software is able to control or influence a hardware MD to administer and/or remove medicinal products, body liquids or other substances to or from the body.

- Rule 12 is applicable to software that does not direct control any hardware MDs, or serve any medical purpose in a standalone manner. For example, transfer of clinical information, display of medical images only, etc. Such devices are not under the listing scope of MDACS.

5.3.3 For SaMD, Rule 9 and Rule 10 are applicable if the intended use is relevant to therapeutic purpose and diagnostic purpose respectively.

5.4 The Technical Documentation for submission shall cover but not limited to the following elements:

5.4.1 Established quality management system (QMS)

5.4.1.1 All MD manufacturers should have a QMS established to ensure the quality of manufacturing of MDs including software MDs. The standard, "ISO 13485 Medical Devices – Quality Management Systems – Requirements for regulatory purposes" or equivalent, has specified and elaborated the requirements of a QMS that could be adopted by MD manufacturers involving in life cycle processes of an MD.

5.4.1.2 The manufacturer shall implement a QMS indicates whether it is a full QMS or a partial system. If it is a partial system, the processes covered and the certification body of the QMS shall be specified.

5.4.2 Essential Principle for safety and performance of medical devices (EP) (Technical Reference TR-004)

5.4.2.1 All MDs, including softwares, shall be ensured that its safety and performance are up to international standards. "Medical Device Administrative Control System Essential Principles Conformity Checklist" (MD-CCL or IVDMD-CCL) demonstrates the basic design and manufacturing requirements of MD. These requirements that are relevant to a particular MDs shall be identified. If requirements are considered not applicable to that particular type of device, the reasons shall be properly recorded and documented.

5.4.2.2 Manufacturers shall be aware of the requirements in our Technical Reference TR-004 for the comprehensive checklist. Where any of these approvals have been obtained on or before 31 December 2004, the Essential Principles Conformity Checklist shall be submitted upon request. Otherwise, the duly completed Essential Principles Conformity Checklist shall also be provided.

5.4.2.3 Alternatively, if the applicants could provide the Essential Requirements / General Safety and Performance Requirements Checklist in accordance with relevant European Union (EU) Medical Device directives or regulations and have sufficient evidence that their products also comply with the MDACS requirements, they may submit the Essential Requirements Checklist and an Essential Principles Declaration of Conformity.

5.4.3 Labelling requirements

5.4.3.1 Device labelling (Physical label, Instruction For Use, User Manuals, etc.) is important information to user to identify the device, so as to communicate safety and performance related matters effectively between stakeholders. It also serves to ensure the traceability of the devices. Information such as, device model and product codes, software versions, are recommended to be presented on the device labelling for proper identification of the software MD.

5.4.3.2 All labelling including instructions, manuals, device and package labels (as specified in the Technical Reference TR-005 Additional Medical Device Labelling Requirements) and Special Listing Information (as specified in the Clause 4.4.13 of Guidance Notes GN-01 Guidance Notes for Overview of the Medical Device Administrative Control System) shall be submitted. However, SaMD may not have physical products which is only be able to download from the internet. Manufacturers shall provide ways for user to obtain the device labelling, such as electronic copies downloaded from website. Applicants shall also provide the corresponding website and demonstrate the procedures,such as screenshots from websites, during submission of listing application of software MD.

5.4.4 Risk management

Risk manangement of software MD is essential to identify and mitigate all foreseeable risks related to the safety and performance of the devices throughout their useful life. In view of the severity and frequency of occurance of the possible risk, manufacturer shall make corresponding remedial actions as far as practicable and evaluate their effectiveness. The principle stipulated in “ISO 14971 Medical Devices — Application of Risk Management to Medical Devices”, or equivalent, should be referenced. For software MDs that contain on network applications, manufacturer shall also be focused on cybersecurity which would be mentioned in Clause 5.5.3.

5.4.5 Clinical evaluation

5.4.5.1 Clinical evaluation is the holistic review of relevant scientific literature and/or the review and assessment of data collected through clinical investigation (please refer to Guidance Notes GN-00 for the definition of clinical investigation). It is a process to establish conformity of the device with the pertinent Essential Principles given in Technical Reference TR-004 and to demonstrate that the device performs as intended by the manufacturer. It establishes the acceptability of risks and side effects when weighed against the intended benefits of the device. The clinical evaluation and its outcome must be documented in a clinical evaluation report

5.4.6 Marketing approval(s) from jurisdictions recognised under MDACS.

5.4.6.1 Applicants shall also provide the marketing approval from any of the GHTF founding members namely Australia, Canada, EU, Japan and the United States of America; and/or Mainland China

The following table summarises the issued documents by MDD and regconised standards (or equivalent) that is/are relevant to the corresponding Technical Documentations.

	MDD issued documents / Regconised standards
Established QMS	ISO 13485 Medical devices - Quality management systems - Requirements for regulatory purposes YY/T 0287 Medical devices - Quality management systems - Requirements for regulatory purposes
Essential Principle for safety and performance of medical devices and relevant Guidance Notes	Guidance Notes GN-02: Guidance Notes for Listing Class II, III & IV General Medical Devices Guidance Notes GN-06: Guidance Notes for Listing Class B, C and D In Vitro Diagnostic Medical Device Technical Reference TR-004: Essential Principles of Safety and Performance of Medical Devices
Labelling requirements	Guidance Notes GN-01: Guidance Notes for Overview of the Medical Device Administrative Control System Technical Reference TR-005: Additional Medical Device Labelling Requirements

	ISO 15223-1 Medical devices – Symbols to be used with medical device labels, labelling and information to be supplied – Part 1: General requirements
Risk management	ISO 14971 Medical devices – Application of risk management to medical devices
Clinical evaluation	ISO 14155 Clinical investigation of medical devices for human subjects – Good clinical practice
Marketing approval(s) from jurisdictions recognised under MDACS	Guidance Notes GN-02: Guidance Notes for Listing Class II, III & IV General Medical Devices Guidance Notes GN-06: Guidance Notes for Listing Class B, C and D In Vitro Diagnostic Medical Device

Please refer to Guidance Notes GN-02 and GN-06 for detailed listing requirements of GMDs and IVDMDs respectively.

5.5 There are also some specific documents required for the Software MDs, including but not limited to:

- Software verification and validation;
- Software versioning and its traceability; and
- Cybersecurity management for device involving wireless or network transmission.

5.5.1 Software verification and validation

5.5.1.1 Besides clinical studies, verification and validation is important process for a software to demonstrate its safety and performance as well as proving to achieve its claimed intended use.

5.5.1.2 In general software development cycle, verification is to ensure the software specification is achieved by provision of an expected outcome from a preset input of data. It allows the manufacturer to make sure the software is designed in accordance with their specification. On the other hand, validation provides evidence which the software has developed according to the intended use and user needs.

5.5.1.3 Applicants are encouraged to refer to international standards such as “IEC 62304 Medical device software – Software life cycle processes” or equivalent standards in order to demonstrate the compliance to the requirements.

5.5.2 Software versioning and its traceability

5.5.2.1 Software versioning is important for tracing in post market events such as adverse events, product complaints or safety alerts, etc. Applicants shall be aware of the version of the software to be listed and the submitted technical documents are equivalent. Please also be advised to have clear identification in the version of the software in the marketing approval document as far as possible.

5.5.2.2 If there is any version update of the software, the Local Responsible Person (LRP) shall submit a change application in accordance with the rquirement under our Guidance Notes GN-10 (Guidance Notes for Changes of Listed Medical Device).

5.5.3 Cybersecurity of medical devices

5.5.3.1 Nowadays, MDs are keen on wireless connection or interconnect through network, such as internet. Risk might be imposed, such as leakage of patient data, during the data transmission through connected devices on the network. Necessary IT security measures and protection shall be considered and implemented throughout the product life cycle in order to avoid vulnerable attacks through network.

5.5.3.2 Foreseeable cybersecurity risks shall be identified and mitigated as far as possible. The manufacturer has the responsibility to assess and manage the cybersecurity risks that could be harmful to the health and safety of a patient, user or any other person. If the application contains any software MDs, the manufacturers are required to address the cybersecurity risks during the useful life of an MD including, but not limited to:

- general considerations, such as the development approach; administration protocols; application of standards; risk management strategies; infrastructure, manufacturing and supply chain management; and provision of information for users;

- technical considerations, such as cyber security penetration testing; modularised design architecture; operating platform security; emerging software; and Trusted access and content provision;

- environmental considerations for the device's intended use, such as connecting to networks, and uploading or downloading data;

- physical considerations, such as mechanical locks on devices and interfaces, physically securing networks, waste management (preventing capture of sensitive paper-based information); and

- social considerations, such as designing out or minimising social-engineering threats (e.g. phishing, impersonation, baiting, tailgating).

5.5.4 Basic cybersecurity requirements

5.5.4.1 A software MD meeting the basic cybersecurity requirements under MDACS shall entail that the manufacturer has:

- considered cybersecurity risks and vulnerabilities as part of an overall risk management process throughout the useful life of an MD.

- taken steps to avoid the use of universal default password. Where passwords are used, the MD passwords shall be unique per device or changed by the user. For pre-installed passwords, they shall be unique per device and sufficiently random. The MD shall be equipped with a mechanism which makes brute force attacks on the device's authentication mechanisms impractical.

- a vulnerability disclosure system in place to manage vulnerability reporting.

- an on-going plan to proactively monitor and identify newly discovered vulnerabilities, and to remediate these vulnerabilities to ensure performance and safety of the device throughout the useful life of an MD.

5.5.5 The above considerations and requirements shall be covered in the Technical Documentations, such as risk management report and other supplementary documents. Since cybersecurity risk can be a concern related to MD safety, consideration and mitigation of risk should also be reflected and in compliance with the EP under MDACS.

5.5.6 Applicants may refer to relevant standards or equivalent, such as, but not limited to:

- ISO 27032 Cybersecurity – Guidelines for Internet Security
- ISO/IEC 27001 Information security, cybersecurity and privacy protection. Information security management systems

5.5.7 Applicants shall also be aware of and follow, if appropriate, the relevant cybersecurity good practices, requirements or recommendations issued by the Office of the Government Chief Information Officer (OGCIO) of the Government of Hong Kong Special Administrative Region of the People's Republic of China.

6. Changes to software medical devices

6.1 Manufacturers and LRP shall evaluate the potential impact of any changes to the function, intended use, essential design, and manufacturing characteristics on the software MDs and its classification (including the classification of the combination of the software MDs with another MD). Proper risk assessment shall also be conducted and addressed in the risk management report if the function or intended use of the software has been affected. The manufacturer shall also perform appropriate validation and verification to the software before releasing it to the market for use.

6.2 Details of the change application procedures and requirements shall refer to Guidance Notes GN-10.

7. Enquiries

7.1 Enquiries concerning this booklet and the MDACS should be directed to:

Medical Device Division,
Department of Health,
Telephone number: 3107 8484
Facsimile number: 3157 1286
Email address: mdd@dh.gov.hk

Website: www.mdd.gov.hk

7.2 Latest versions of the Guidance Notes for the MDACS and the application forms for listing are available at the website: https://www.mdd.gov.hk

8. References

8.1 International Medical Device Regulators Forum. Software as a Medical Device (SaMD): Key Definitions.

8.2 International Medical Device Regulators Forum. SaMD WG N12 - Software as a Medical Device: Possible Framework for Risk Categorization and Corresponding Considerations.

8.3 International Medical Device Regulators Forum. Software as a Medical Device (SaMD): Application of Quality Management System.

8.4 International Medical Device Regulators Forum. Software as a Medical Device (SaMD): Clinical Evaluation.

8.5 Department of Health. Guidance Notes for Definitions and Abbreviations for Medical Device Administrative Control System. Guidance Notes GN-00.

8.6 Department of Health. Guidance Notes for Overview of the Medical Device Administrative Control System. Guidance Notes GN-01.

8.7 Department of Health. Guidance Notes for Listing Class II/III/IV General Medical Devices. Guidance Notes GN-02.

8.8 Department of Health. Guidance Notes for Listing Class B, C and D In Vitro Diagnostic Medical Devices. Guidance Notes GN-06.

8.9 Department of Health. Guidance Notes on Changes for Listed Medical Devices. Guidance Notes GN-10.

8.10 Department of Health. Classification of General Medical Devices. Technical Reference TR-003.

8.11 Department of Health. Essential Principles of Safety and Performance of Medical Devices. Technical Reference TR-004.

8.12 Department of Health. Classification of In Vitro Diagnostic (IVD) Medical Devices. Technical Reference TR-006.

8.13 ISO 13485:2016 Quality management system – Requirements for regulatory purposes.

8.14 ISO 14971:2019 Medical devices – Application of risk management to medical devices.

8.15 ISO 14155:2020 Clinical investigation of medical devices for human subjects – Good clinical practice.

8.16 ISO 15223-1:2021 Medical devices – Symbols to be used with medical device labels, labelling and information to be supplied. Part 1: General Requirements.

8.17 IEC 62304:2006 Medical device software – Software life cycle processes.

8.18 ISO 27032:2012 Cybersecurity – Guidelines for Internet Security.

8.19 ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. Information security management systems.

8.20 Health Sciences Authority. Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach. Rev.2.0. 2022.04.

8.21 Cyber Security Agency of Singapore. Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)] Publication No. 2 – Scehme Specifications. Version 0.5. 2023.10.

8.22 Therapeutic Goods Administration. Medical device cyber security guidance for industry.

8.23 National Medical Products Administration. Guidelines for registration of medical device software.

8.24 National Medical Products Administration. Guidelines for registration of medical device cybersecurity.

8.25 Medical Device Coordination Group. MDCG 2019-11, Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR.

8.26 Medical Device Coordination Group. MDCG 2019-16, Guidance on Cybersecurity for medical devices.