CCC SP-153-4

Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)] Publication No. 4

Assessment Methodology

October 2024
Version 1.0

FOREWORD

The Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)] is part of efforts from the Ministry of Health (MOH), Cyber Security Agency (CSA), Health Sciences Authority (HSA), and Synapxe to better secure Singapore's cyberspace and to raise cyber hygiene levels in medical devices.

Under the CLS(MD), the cybersecurity label for medical devices would provide an indication of the level of security in medical devices. It aims to improve security awareness by making such provisions more transparent to healthcare users and empowers them to make informed purchasing decisions for medical devices with better security using the information on the cybersecurity label.

The CLS(MD) seeks to incentivise manufacturers to develop and provide medical devices with enhanced cybersecurity provisions. The labels also serve to differentiate medical devices with better cybersecurity safeguards in the market, from their competitors.

At the same time, CSA intends to engage other like-minded partners for mutual recognition of the CLS(MD) with the objective of eliminating duplicated assessments across national boundaries.

The CLS(MD) is managed by the Cybersecurity Certification Centre (CCC) and jointly owned under the ambit of the Cyber Security Agency of Singapore (CSA) and Ministry of Health (MOH).

AMENDMENT RECORD

Version	Date	Author	Changes
0.3	October 2023	Cyber Security Agency of Singapore	Draft
0.4	April 2024	Cyber Security Agency of Singapore	Draft
1.0	October 2024	Cyber Security Agency of Singapore	Release

CONTENTS

INTRODUCTION

This document specifies the assessment methodology for the Security Baseline Requirements and the Enhanced Security Requirements under the Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)].

INTENDED USAGE

The assessment methodology seeks to provide clarification on the requirements and expectations for each of the security provisions of the CLS(MD).

Each security provision is structured in the following manner:

- **Intent of the Security Provision** – Explains the objective and intention behind the security provision.
- **Minimum Requirements** – Specifies what is required of either the manufacturer or the medical device to fulfil the security provision.
- **Supporting Evidence** – Provides examples and/or suggestions of the expected supporting evidence that shall be provided by the manufacturer to allow the assessor to determine if the security provision is fulfilled.
- **Assessment** – Specifies how the assessor shall check or examine the supporting evidence to determine if a security provision is fulfilled.
    - "**Check**" – Assessor will generate a verdict by performing simple comparison or straightforward verification of completeness.
    - "**Examine**" – Assessor will generate a verdict by performing a more thorough detailed analysis.

PROVISIONS FOR EACH CLS(MD) LEVEL

Table 1 details the mandatory provisions per each CLS(MD) level.

CLS(MD) Levels	Requirements	Assessment	Mandatory Provisions
Level 1	Security Baseline Requirements	Manufacturer's Declaration of Conformity	VDP.1, CSUP.1, CSUP.4, PAUT.3, PAUT.4, RDMP.1
Level 2, 3, 4	Enhanced Security Requirements		All security provisions as defined within this document.

Table 1 - Mandatory Provisions for each CLS(MD) Level

APPLICABILITY OF PROVISIONS

The provisions set forth in this document have been specifically selected to address and mitigate risks to medical devices arising from potential attack vectors.

These provisions are mandatory and shall be applicable to the medical device, unless it can be demonstrated that the attack vector that the provision is seeking to address is not present on the medical device.

Examples of Applicability Determination

1) In cases where the medical device under evaluation does not possess the capability to support remote sessions, provision RMOT.1 may be deemed "Not Applicable". This determination is based on the absence of the attack vector associated with remote session functionality. Consequently, the medical device shall not be required to meet the requirements specified in RMOT.1.
2) Conversely, if the medical device under evaluation stores sensitive information, such as Personally Identifiable Information (PII), provision STCF.1 shall be deemed "Applicable". This determination is based on the presence of the attack vector associated with the storage of sensitive data. To comply with the requirements of STCF.1, the medical device shall implement encryption to protect the confidentiality of the stored sensitive data. If the device is unable to support encryption due to technical limitations or other constraints, the provision shall be considered unmet.

Documentation Requirements for Inapplicable Provisions

In cases where a provision is deemed inapplicable to the medical device, the following shall be provided:

1) A detailed justification explaining the inapplicability of the provision to the medical device.
2) Supporting evidence demonstrating that the attack vector corresponding to the security provision is not present in the medical device.

TERMS AND DEFINITIONS

Term	Definition
Sensitive Data	Sensitive data refers to any information that, if disclosed, altered, or accessed by unauthorized parties, could result in significant harm to individuals, organizations, or systems. Examples: Sensitive Security Parameters, Critical Security Parameters, Personally Identifiable Information (PII), clinical data.
Critical Security Parameters	Critical security parameters used for integrity and authenticity checks of software updates shall be unique per device. Example: secret keys, private components of certificates, etc.
Sensitive Security Parameters	These are parameters that are used to authentication users with the device's interfaces, typically allowing the user to perform administrative actions that if abused, could be detrimental. Examples: Admin password, Wi-Fi password (SSID), device's private key for client authentication, root key used to encrypt other sensitive parameters, digital signature public key, etc.
Personally Identifiable Information	This refers to any information that can be used to identify, contact, or locate an individual. Examples: Full Name, Address, Email Address, Phone Number, Passport Number, Biometric data, etc.
Clinical Data	This refers to sensitive and confidential information related to an individual's medical history, treatment, and health records. Examples: Electronic Health Records (EHR), Laboratory test results, Physician Notes, Medical history, Prescription records, etc.
Authentication Interface	Interfaces on the device (or its companion application/services) that requires user interaction for authentication. Examples: WebGUI login portal, Mobile application login page, etc.
Authentication Mechanisms	Credential that is utilised by the user to authenticate themselves to the device using an authentication interface. Examples: passwords, tokens, smart cards, digital signatures, biometrics, etc.

Hard-coded	Embedding data directly into the source code of a program. Examples: hard-coded unique per device identifiers, hard-coded critical security parameters, etc.
LDAP	An open standard protocol that is commonly used to communicate with directory servers.
COTS	COTS refers to 'Commercial off the shelf' products which are packaged or canned (ready-made) hardware or software. These products are adapted aftermarket to the needs of the purchasing organization, rather than the commissioning of custom-made, or bespoke, solutions
Operating System	An operating system (OS) is system software that manages computer hardware and software resources and provides common services for computer programs. Examples of Operating Systems not limited to the following: - Microsoft Windows - Linux - Real-time operating systems (e.g., FreeRTOS, SafeRTOS, VxWorks, Nucleus, QNX, etc.).
Access Control Mechanisms	Security measures that regulate and manage access to resources, systems, or data within an organization's environment. Examples: Access control list (ACLs), role-based access control (RBAC) or multi-factor authentication (MFA).
Threat Risk Assessment	The systematic evaluation of potential threats and associated risks to an organization's information systems, networks, and data. This process helps identify and prioritize potential threats, vulnerabilities, and the potential impact of security incidents.
Anti-malware Software	Software designed to detect, prevent, and remove malicious software, such as viruses, worms, and ransomware, from computer systems and networks, thereby enhancing cybersecurity protection. Examples: Antivirus software, anti-spyware software or endpoint detection and response (EDR) solutions.
Software Restoration	The process of returning a software application, system, or environment to a previous state or version after it has been compromised, experienced a failure, or undergone undesirable changes.

Table 2 – Terms and Definitions

ABBREVIATIONS

The following acronyms are used in this publication:

CCC	Cybersecurity Certification Centre
CSA	Cyber Security Agency of Singapore
CVE	Common Vulnerabilities and Exposures
DUT	Device Under Test
HSA	Health Sciences Authority
LDAP	Lightweight directory access protocol
MAC	Media Access Control Address
MFA	Mult-Factor Authentication
PII	Personal Identifiable Information
SMDR	Singapore Medical Device Register
TRA	Threat Risk Assessment
VDP	Vulnerability Disclosure Process
SOP	Standard Operating Procedure

VULNERABILITY DISCLOSURE POLICY (VDP)

VDP.1

The manufacturer shall provide an avenue for the reporting of vulnerabilities.

Note: This provision is taken to be fulfilled if the medical device has been listed by the Health Sciences Authority (HSA) in either the Class A Medical Device Database or in the Singapore Medical Device Register (SMDR).

Intent of the Provision

The intent of this provision is to ensure that medical device owners/operators can report vulnerabilities to the manufacturers and that processes exist to communicate remediation to affected stakeholders.

Minimum Requirements

- Manufacturers shall have a formalised process to:
  - Receive information from vulnerability finders (e.g., web forms, contact information, support hotlines, emails, etc.).
  - Disclose vulnerabilities that are found on the medical device.
  - Propose remediation to affected stakeholders.

NOTE: It is recommended that the manufacturer establish and maintain a publicly accessible vulnerability disclosure policy (referencing the ISO/IEC 29147 [1]*) as part of their formalised process. Such a policy helps to delineate clear rules of engagement for security researchers and establish a comprehensive communication framework for the reporting of vulnerabilities by all relevant parties. The vulnerability disclosure policy should be readily available to the public and is recommended to include, but not be limited to the following components:*

- *Contact information for reporting of vulnerabilities;*
- *Clear instructions on how vulnerabilities can be reported;*
- *Clear expectation for the timeline, including initial acknowledgement of receipt (e.g., within 7 working days) and regular status updates until the vulnerability is resolved.*

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., contact information, support emails, support hotlines, etc.) to demonstrate that medical device owners/operators can contact the manufacturer to report vulnerabilities.
2) The manufacturer shall describe the processes to:
   - Gather information from vulnerability finders.
   - Disclose the existence of vulnerabilities on the medical device.
   - Propose remediation to affected stakeholders.

Assessment

- The assessor shall check that there is a way for medical device owners/operators to report vulnerabilities to the manufacturer.
- The assessor shall check that there are processes in place to gather information from vulnerability finders, disclose the existence of vulnerabilities and propose remediation to affected stakeholders.

MANAGEMENT OF SENSITIVE DATA (MSD)

MSD.1

The manufacturer shall maintain a list of sensitive data (such as personal identifiable information) that is collected and transmitted/transferred by the medical device.

Intent of the Provision

The intent of this security provision is to ensure that the manufacturer accounts for all sensitive data collected or transmitted/transferred by the medical device.

Minimum Requirements

- All sensitive data that is collected or transmitted/transferred by the medical device shall be accounted for.
- The device shall only collect or transmit/transfer sensitive data when necessary.

Sensitive data is defined as the following:

- Personally Identifiable Information (e.g., Patient's full name, home address, national identification numbers, phone numbers, email addresses, etc.).
- Clinical Data (e.g., Patient's health and medical history, etc.).
- Sensitive or Critical Security Parameters (e.g., cryptographic keys, digital certificates, access control lists, authentication tokens, login credentials, etc.).

Supporting Evidence

1) The manufacturer shall provide a list of all sensitive data collected by the medical device.
    a. Where applicable, the manufacturer shall also clearly specify the sensitive data being transmitted or transferred and its destination (e.g., back up to a database, stored on remote server, stored on removable storage, etc.).
2) For all sensitive data listed in (1), the manufacturer shall explain the necessity of its the collection and transmission (e.g., Patient name is collected by the medical device as part of the initial registration process, etc.).
3) In cases where the medical device neither collects nor transmits/transfers sensitive data, the manufacturer shall provide a declaration to this effect.

Assessment

- The assessor shall examine the evidence provided by the manufacturer to determine that all sensitive data collected or transmitted/transferred by the medical device is properly accounted for and deemed necessary for its operation.

AUDIT CONTROLS (AUDT)

AUDT.1

The medical device logs or audit trails shall not store sensitive data in clear text.

Intent of the Provision

The intent of this security provision is to ensure that logs or audit trails generated by the medical device, intended to support investigations, audits, or forensic analysis in the event of cybersecurity incidents, do not contain sensitive information in clear text.

Minimum Requirements

- The medical device shall be able to capture and store device logs and/or audit trails.
- In all logs and/or audit trails generated by the medical device, it shall not store contain sensitive information in clear text.

Supporting Evidence

1) The manufacturer shall provide samples of logs and/or audit trails that are generated by the medical device.
2) If the logs and/or audit trails generated by the device contains sensitive information, the manufacturer shall provide a description of the measure(s) implemented (e.g., masking, encryption, pseudonymization, etc.) to ensure that such information is not stored in clear text

Assessment

- The assessor shall check and verify that the medical device has the capability to capture and store logs or audit trails.
- The assessor shall check the provided logs and/or audit trails to verify that they do not contain sensitive information.

AUDT.2

The medical device shall be capable of logging security-related actions and activities performed on it.

Intent of the Provision

The intent of this security provision is to ensure that security-related actions and activities are logged to support investigations, audits, and forensic analysis in the event of a cybersecurity incident.

Minimum Requirements

- The medical device shall have the capability to capture security-relevant actions and activities to facilitate investigations, audits, and forensic analysis.

Examples of actions and activities that should be logged are, but not limited to:

- Operating System Events (i.e., Start-up and shut down, information on system/services, network connection changes, attempts to change security settings, etc.).
- User Account Information (i.e., successful, and unsuccessful login or logoff attempts, user account changes, use of privileges, etc.).
- Companion Application Operations (i.e., application start-up, shut down, login failures, transactions, etc.).

Supporting Evidence

1) The manufacturer shall provide a comprehensive list of all security-relevant actions and activities logged within the medical device generated logs or audit trails.

Assessment

- The assessor shall examine the provided logs and/or audit trails to determine that the medical device captures the security-relevant actions and activities as specified by the manufacturer.

AUTHORISATION (AUTH)

AUTH.1

Access to the medical device's functionalities and resources shall be restricted to authorised users, ensuring individuals can only access what their permissions allow.

Intent of the Provision

The intent of this security provision is to ensure that the medical device grants access only to the functionalities and resources that users are authorised to access.

Minimum Requirements

- After the user is authenticated, the medical device shall be capable of restricting access to its functionalities and resources based on the user's authorised permissions.
- The medical device shall only include pre-installed privileged users and roles (e.g., Administrator, Guest/Demo, Technical Support, Service accounts, etc.) that are necessary for operation.

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., screenshots, device documentation, etc.) demonstrating the medical device's ability to restrict access to functionalities and resources based on the defined user permissions.
2) The manufacturer shall provide a list of pre-installed users and roles, along with a rationale explaining the necessity of each.

Assessment

- The assessor shall examine the evidence to determine that the medical device can restrict access to functionalities and resources based on the user permissions.
- The assessor shall examine the list of pre-installed users and roles, along with the provided rationale, to determine their necessity.

AUTH.2

Authorised users shall be able to assign and segregate different roles (i.e., user, administrator and/or service accounts) on the medical device.

Intent of the Provision

The intent of this security provision is to ensure that the medical device supports the assignment and segregation of different roles and their respective privileges.

Minimum Requirements

- The medical device shall be capable of supporting access control mechanisms (e.g., defining roles, creating user groups, and setting rule-based policies, etc.).
- The medical device shall be capable of allowing authorised users (e.g., system administrators, field support engineers, etc.) to manage and assign roles and privileges to other users.

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., screenshots, videos, device documentations, etc.) demonstrating how the medical device supports access control mechanisms.
2) The manufacturer shall provide evidence (e.g., screenshots, videos, device documentations, etc.) demonstrating how authorised users can manage and assign roles and privileges to other users.

Assessment

- The assessor shall examine the evidence to determine that the medical device supports access control mechanisms.
- The assessor shall examine the evidence to determine that authorised users are able to manage and assign roles and privileges to other users.

CYBER SECURITY PRODUCT UPGRADES (CSUP)

CSUP.1

Manufacturers shall have an on-going plan to remediate cybersecurity vulnerabilities to ensure that the performance and safety of the medical device is not compromised throughout its lifecycle.

Note: This provision is taken to be fulfilled if the medical device has been listed by the Health Sciences Authority (HSA) in either the Class A Medical Device Database or in the Singapore Medical Device Register (SMDR).

Intent of the Provision

The intent of this provision is to ensure that the manufacturer has a plan to address cybersecurity vulnerabilities, maintaining the medical device's performance and safety.

Minimum Requirements

- The manufacturer shall have a plan to develop and test fixes (e.g., patches, updates, etc.) to address vulnerabilities that are verified to impact the medical device.

Supporting Evidence

1) The manufacturer shall provide supporting evidence (e.g., documentation, etc.) demonstrating the existence of a plan to develop and text fixes for vulnerabilities that are verified to impact the medical device.

Assessment

- The assessor shall examine the evidence to determine that the manufacturer has a plan in place to address vulnerabilities that are verified to impact the medical device.

CSUP.2

Manufacturers shall have a process in place to notify and guide medical device owners/operators on how to successfully perform software updates through instruction manuals and installation procedures.

Intent of the Provision

The intent of this provision is to ensure that the manufacturer has a clear process or procedure to notify and guide medical device owners/operators on the installation of software updates.

Minimum Requirements

- The manufacturer shall have a process or procedure to notify medical device owners/operators when a software update becomes available.
- If software updates are **performed by the manufacturer's representatives** (e.g., field support engineers), a standardised process and procedure must be in place for them to follow.
- The software update guidance, process, and procedures shall be clear and easy to understand to ensure proper installation of updates.

These requirements are applicable to software updates for the following:

- Device's Operating Systems
- Device's Drivers and Firmware
- Device's Anti-Malware Software
- Other components in the device (e.g., asset management software, license management software, etc.).

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., screenshots, user manuals, etc.) demonstrating how medical device owners/operators are notified of new software updates.

2) The manufacturer shall provide the software update guidance (e.g., instruction manuals, installation guides, etc.) provided to medical device owners/operators.

3) If software updates are performed by the manufacturer's representatives, the manufacturer shall provide evidence (e.g., SOPs, installation guides, etc.) demonstrating that a standardised process or procedure is followed during the installation.

   NOTE: The evidence in (2) and (3) shall be device-specific, explicitly referencing the device under test and shall also clearly detail the steps (e.g., use of certain commands, button presses, etc.) that a manufacturer's representative follows when installing software updates.

Assessment

- The assessor shall examine the evidence to determine that the manufacturer has procedures in place to notify medical device owners/operators of available software updates.

- The assessor shall examine the software update guidance documents to determine that they are clear and easily understandable for the proper installation of software updates.

- The assessor shall examine the evidence (e.g., SOPs, installation guides, instruction manuals, etc.) to determine that the manufacturer has a standardised process and procedure for their representatives to follow when installation software updates on the medical device.

CSUP.3

The device shall only allow the installation of approved software.

Intent of the Provision

The intent of this provision is to ensure that the medical device has the capability to prevent the installation of unapproved software and/or applications.

Minimum Requirements

- The medical device shall have the capability to prevent the installation of unapproved software and/or applications.

Possible examples of how the medical device can prevent the installation of unapproved software and/or applications, but are not limited to:

- The medical device only allows the installation of approved software/application by using application whitelisting or digital code signing.
- The medical device uses privilege controls to prevent unauthorised users from installing unapproved software.
- The medical device completely blocks the installation of any software by disabling all external ports and interfaces, or by write-protecting the medical device's storage medium.

Supporting Evidence

1) The manufacturer shall provide an explanation of how the medical device prevents the installation of unapproved software.
2) The manufacturer shall provide evidence (e.g., screenshots, videos, device documentation, etc.) demonstrating the mechanism that prevents the installation of unapproved software and/or applications.

- NOTE: Test results or device-specific technical documentation demonstrating the device's capability to prevent the installation of unapproved software and/or applications are accepted.

Assessment

- The assessor shall examine the evidence to determine that the medical device has the capability to prevent the installation of unapproved software and/or application.

CSUP.4

The manufacturer shall have an ongoing plan to proactively monitor and identify newly discovered cybersecurity vulnerabilities, assess their threat level, and respond accordingly.

Note: This provision is taken to be fulfilled if the medical device has been listed by the Health Sciences Authority (HSA) in either the Class A Medical Device Database or in the Singapore Medical Device Register (SMDR).

Intent of the Provision

The intent of this provision is to ensure that the manufacturer has a plan in place to regularly monitor, identify, and assess vulnerabilities in the medical device.

Minimum Requirements

- The manufacturer shall have processes in place to monitor relevant sources (e.g., CVE databases such as the CVE List, NVD, ISACs/ISAOs, etc.) to proactively identify vulnerabilities that may affect the medical device.
- There shall be a process to verify if the medical device is vulnerable to the identified potential threats.
- For all verified vulnerabilities, the manufacturer must perform a Threat and Risk Assessment (TRA) to determine their potential impact and assign an appropriate severity rating (e.g., critical, high, medium, low).

Supporting Evidence

1) The manufacturer shall provide the sources that are actively monitored to identify vulnerabilities relevant to the medical device.
2) The manufacturer shall provide supporting evidence (e.g., internal process documents, etc.) demonstrating the process used to verify whether the medical device is impacted by the identified vulnerabilities.
3) The manufacturer shall provide supporting evidence (e.g., internal process documents, etc.) demonstrating the process for conducting TRA on verified vulnerabilities identified in (2).
4) The manufacturer shall provide the severity ratings (e.g., critical, high, medium, low, etc.) used to categorise vulnerabilities.

Assessment

- The assessor shall check that the manufacturer has processes in place to monitor relevant sources and proactively identify vulnerabilities that may impact the medical device.
- The assessor shall check that the manufacturer has a process to assess whether the device is susceptible to identified vulnerabilities.
- The assessor shall check that the manufacturer has processes in place to perform TRA on verified vulnerabilities and that they are categorised into severity ratings.

DATA BACKUP AND DISASTER RECOVERY (DTBK)

DTBK.1

For medical devices that handle data required for further processing or storage, it shall provide the capability to back up this data to remote storage or removable media.

Intent of the Provision

The intent of this security provision is to ensure that the medical device has the capability to back up data required for further processing or storage to remote storage or removable media.

Minimum Requirements

- The medical device shall have the capability to back up data needed for further processing or storage to remote storage or removable media.

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., product documentation, videos, etc.) demonstrating the medical device's ability to back up required for further processing or storage to remote storage or removable media.

Assessment

- The assessor shall check that the medical device has the capability to back up data to remote storage or removable media.

DTBK.2

The medical device shall be able to back up system configuration information and perform patch or software restoration.

Intent of the Provision

The intent of this security provision is to ensure that the medical device can back up system configuration information and support patch and software restoration. These capabilities are essential to ensure the continuity of the device's operation in the event of software corruption, malfunction, or compromise, thereby minimising downtime.

Minimum Requirements

- The medical device shall have the capability to back up system configuration and perform patch or software restoration.

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., product documentation, screenshots, etc.) demonstrating the medical device's ability to back up system configuration information.

2) The manufacturer shall provide evidence (e.g., product documentation, screenshots, etc.) demonstrating the medical device's ability to perform patch and software restoration.

Assessment

- The assessor shall check that the device has the capability to back up system configuration information.

- The assessor shall check that the device can perform patch and software restoration.

MALWARE DETECTION/PROTECTION (MLDP)

MLDP.1

The medical device shall implement at least one malware protection measure of mechanism.

Intent of the Provision

The intent of this security provision is to ensure that the medical device has at least one malware protection measure or mechanism in place.

Minimum Requirements

- The medical device shall implement at least one malware protection measure or mechanism.

Possible examples of malware protection measures/mechanisms include, but not limited to:

- Anti-malware software.
- Secure boot.
- Host-based intrusion detection and/or prevention software.
- Application whitelisting.

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., screenshots, videos, device documentation, etc.) demonstrating the implementation of the medical device's malware protection measure or mechanism.
    a. If the medical device uses anti-malware software, the name and version number shall be provided.
2) The manufacturer shall explain how the malware protection measure or mechanism is sufficient to protect the medical device from malware.

Assessment

- The assessor shall examine the supporting evidence to determine that the manufacturer has implemented a malware protection measure or mechanism on the medical device.
- The assessor shall examine the malware protection measure(s) or mechanism(s) to determine the adequacy of these measures in protecting the medical device against malware.

NODE AUTHENTICATION (NAUT)

NAUT.1

The medical device shall implement a network access control measure or mechanism.

Intent of the Provision

The intent of this security provision is to ensure that the medical device only allows network access to authorised entities (such as services, other devices, etc.).

Minimum Requirements

- The medical device shall have the capability to only allow access to authorised entities (such as services, other devices, etc.).

Possible examples of such capabilities include, but not limited to:

- Internal firewalls.
- Network connection whitelists.
- Peer service/device using credentials or certificates.
- Policies that allow communication only with authenticated devices.

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., screenshots, videos, device documentation, etc.) demonstrating the implementation of the medical device's network access control measure or mechanism.

2) The manufacturer shall explain how the network access control or measure is sufficient to ensure that only authorised entities have access to the network.

Assessment

- The assessor shall check the evidence to verify that the manufacturer has implemented a network control measure or mechanism on the medical device.

  The assessor shall examine the supporting evidence to determine the adequacy of these measure(s) or mechanism(s) in restricting access only to authorised entities.

CONNECTIVITY CAPABILITIES (CONN)

CONN.1

All communication channels supported by the medical device shall be declared by the manufacturer.

Intent of the Provision

The intent of this provision is to ensure that the manufacturer declares all communication channels supported by the medical device.

Minimum Requirements

- All supported communication channels shall be accounted for, including those not intended for direct user interaction (e.g., communication channels that are used for automatic updates, field support services, etc.), physical network interfaces, and interfaces that are disabled by default.

Possible examples of communication channels supported by the medical device include, but not limited to:

- Wi-Fi
- Bluetooth
- ZigBee
- LoRaWAN
- NFC
- Cellular (3G/4G/5G)
- Ethernet

Supporting Evidence

1) The manufacturer shall provide a comprehensive list of all communication channels supported by the medical device, clearly indicating whether each channel is enabled or disabled by default.

Assessment

- The assessor shall examine the list to determine if it is complete. The assessment may be further supported by insights gained from evaluating other security provisions and supporting evidence outlined in this document.

PERSON AUTHENTICATION (PAUT)

PAUT.1

The medical device shall support and enforce authentication for all users and roles.

Minimum Requirements

- The manufacturer shall state the functionalities that are available on the medical device without authentication.

  NOTE: Where applicable, the medical device may allow medical functionalities (e.g., patient monitoring, handling of medical emergencies, etc.) without authentication, if necessary for its intended use.

Supporting Evidence

1) The manufacturer shall provide a list of the medical device's functionalities that are available without authentication, along with a rationale explaining why authentication is not required for those functionalities.

Assessment

- The assessor shall examine the list of functionalities that do not require authentication and the rationale to determine that authentication is not necessary for those specific functionalities.

PAUT.2

The medical device shall support the ability to change authentication values (e.g., passwords, PINs, biometrics, etc.) for all users and roles.

Intent of the Provision

The intent of this provision is to ensure that the medical device provides the capability for device owners/operators to change authentication values for all users and roles.

Minimum Requirements

- The device shall have the capability to change the authentication values for all users and roles.
- If the process of changing authentication values is not easily understandable or straightforward (e.g., requiring the use of command prompts, terminal, coding, etc.), comprehensive guidance shall be provided to the medical device owner/operator to assist in the process.

Supporting Evidence

1) For authentication interface indicated in PAUT.1, the manufacturer shall provide evidence (e.g., screenshots, videos, user guidance documents, device documentations, etc.) demonstrating how medical device owners/operators can change the authentication values for all users and roles.
2) If the process of changing authentication values is not easily understandable or straightforward, the manufacturer shall provide evidence (e.g., user guidance documents, videos, online guides, etc.) to show that comprehensive guidance is provided to assist medical device owners/operators in changing authentication values for all users and roles.

Assessment

- The assessor shall check the evidence to verify that the medical device supports the changing authentication values for all users and roles.
- If the process is not easily understandable or straightforward, the assessor shall check the evidence to verify that comprehensive guidance is provided to medical device owners/operators for changing authentication values.

PAUT.3

In any state other than the factory default, medical device passwords shall be unique per device or user defined.

If factory pre-installed passwords are unique per device, they must be generated using a mechanism that mitigates the risk of automated attacks targeting a class or type of device.

Intent of the Provision

The intent of this provision is to ensure that best practices are adopted with regards to pre-installed passwords on the medical device.

Minimum Requirements

- The medical device shall perform user authentication.
- If pre-installed passwords are used, they must comply with the requirements outlined in the table below.

  NOTE: For medical devices that incorporate a computer with an operating system (e.g., Windows, Linux), **the security credentials at the operating system level shall meet all the requirements specified in this provision**. This requirement extends to, but is not limited to:

  - Standard User Accounts
  - Administrator Accounts
  - Service Accounts

  NOTE: The security requirements of this provision are also applicable to medical devices designed to operate in Kiosk Mode operating systems.

  NOTE: The authentication process shall **require the use of credentials** (e.g., username, passwords or equivalent secure authentication factors). Merely supporting authentication without implementing credential-based access does not meet the requirements of this provision.

  - Example: A medical device that allows users to bypass login or use a default guest account does not meet the requirement, as it fails to enforce credential-based authentication for accessing the medical device.

Pre-Installed Passwords/PINs-type specific requirements:

Pre-Installed Passwords/PINs that are unique per device	• Pre-installed passwords/PINs shall be different across different units of the same device model. • Pre-installed passwords/PINs shall be randomised using a random function. • Pre-installed passwords/PINs shall not be relatable in an obvious manner to publicly available information regarding the device (e.g., Wi-Fi SSID, MAC address, product serial number, etc.). • Pre-installed passwords/PINs shall not have incremental counters (e.g., “password1”, “password2”, “password3”, etc.). • Pre-installed passwords/PINs shall not have common strings or patterns (e.g., “Password123”, “QWERTY”, etc.).
Pre-installed passwords/PINs that are not unique	• The user shall be required to define a new password/PIN upon the device’s initialisation. The device shall not enter the operationalised state before the pre-installed password/PIN is changed.
No pre-installed passwords/PINs	• The user shall be required to define a new password/PIN upon the device’s initialisation. The device shall not enter the operationalised state before the pre-installed password/PIN is changed.

- Authentication shall be performed over a secure communication channel. Acceptable examples include, but are not limited to:
  - TLS 1.2 or higher, with acceptable cipher suites (refer to NIST SP 800-52 [2]).
  - SSH-2 or higher, with acceptable cryptographic algorithms and key lengths (refer to NIST SP 800-131 [3]).
  - For devices that use Bluetooth or Bluetooth Low Energy (BLE), Security Mode 1 with Security Level 3 or higher can be used (excluding Security Mode 2 with Security Level 1).

Supporting Evidence

1) The manufacturer shall provide a list of all authentication interfaces that are enabled by default (e.g., device administrator portal, companion mobile application, telnet, FTP, SSH, etc.) and categorise the corresponding passwords/PINs as follows:
    a. Pre-installed passwords/PINs that are unique per device.
    b. Pre-installed passwords/PINs that are not unique per device.
    c. No pre-installed passwords/PINs.
2) For pre-installed passwords/PINs that are Unique per Device:
    a. The manufacturer shall describe the password/PIN generation method(s) used to randomise pre-installed passwords/PINs (e.g., cryptographically secure pseudorandom number generator, random function etc.).
    b. The manufacturer shall provide 10 sample passwords generated using the described method in (2a).
3) For pre-installed passwords/PINs that are Not Unique:
    a. The manufacturer shall provide supporting evidence (e.g., user manuals, screenshots, videos, etc.) showing that the medical device setup process does not allow it to enter an operational state until a new password/PIN is defined.
4) No pre-installed passwords/PINs:
    a. The manufacturer shall provide supporting evidence (e.g., user manuals, screenshots, videos, etc.) showing that the medical device setup process does not allow it to enter an operational state until a new password/PIN is defined.
5) The manufacturer shall provide evidence to demonstrate the secure transmission of credentials using best practice cryptography.
    a. For TLS Implementations, refer to ANNEX A – **Annex A** for more information.

Assessment

- The assessor shall check and verify that the list of authentication interfaces enabled by default is complete and that all passwords/PINs are categorised accordingly.
- For pre-installed passwords/PINs that are Unique per Device, the assessor shall check/examine the following:
  - They are not relatable in an obvious manner to publicly available information, do not have incremental counters and do not have common string or patterns.
  - That the password/PIN generation method(s) used are appropriate to sufficiently randomise generated passwords/PINs.
- For pre-installed passwords/PINs that are not unique, the assessor shall check/examine the following:
  - That the supporting evidence provided by the manufacturer shows that the device will not enter an operationalised state until a new password/PIN is defined.
- If no pre-installed passwords/PINs are used, the assessor shall examine the evidence to verify that the device will not enter an operationalised state until a new password/PIN is defined.
- The assessor shall examine the evidence to determine that credentials are transmitted securely using best practice cryptography.

PAUT.4

The medical device shall be designed to make successful brute-force attacks on its authentication interfaces impractical.

Intent of the Provision

The intent of this provision is to ensure that the medical device implements measures to prevent successful brute-force attacks on its authentication interfaces.

Minimum Requirements

- All authentication interfaces on the medical device (e.g., device administrator portal, companion mobile application, OS-level account authentication, FTP, SSH, etc) shall employ a brute-force attack prevention measure. Examples of typical brute-force prevention measures include, but not limited to:
  - Rate limiting policies that restrict the number of authentications within an interval (e.g., locks/delays enforced after a threshold is met, etc.).
  - Multi-factor authentication (MFA) after initial setup.
  - CAPTCHA to ensure logins are attempts are not automated.
  - Requiring One-Time-Passwords/PINs (OTPs).
  - Account lockout until hardware reset is performed.
  - Account lockout until re-enabled through a webGUI admin portal.

- NOTE: For medical devices that incorporate a computer with an operating system (e.g., Windows, Linux), the **authentication interfaces at the operating system level shall meet all the requirements of this security provision.** This also applies to medical devices that are intended to be operated in Kiosk Mode.

- If a rate limiting policy is implemented as the brute-force attack prevention measure, it shall, meet the following criteria:
  - When a delay is enforced after a user exceeds the predefined number of failed login attempts, the system shall ensure that it would take **at least 100 days** for a brute-force attack to succeed.
  - If IP blocking is enforced, the chance of a successful brute-force attack shall be **lower than 1%.**

    NOTE: Refer to the formulas provided below in the Supporting Evidence section to perform the appropriate calculation.

- **Alternatively**, if the medical device does not have brute-force prevention mechanisms on its authentication interfaces, it shall implement measures that mitigate typical brute-force attack vectors, such as:

  - Requiring physical presence for authentication.
  - Ensuring that logical brute-force attacks are inapplicable (e.g., device operates in a fully air-gapped environments or has no network connectivity, etc).
  - Disabling or restricting access to physical ports (e.g., USB, SD card, serial ports) by design (e.g., ports located within an internal compartment requiring cover removal or special tools for access).

    NOTE: If USB ports are required for functions such as data backup, they must include safeguards to prevent to use of Human Input Devices (HIDs) such as mice or keyboards. Additionally, the medical device must have mechanisms to prevent the execution of unauthorised scripts.

Supporting Evidence

1) The manufacturer shall provide a list of all authentication interfaces (e.g., device configuration web portal, companion mobile application, software application login, etc.) along with the corresponding authentication mechanism (e.g., passwords, tokens, digital signatures, biometrics, etc.).
2) The manufacturer shall describe the brute-force prevention measure implemented on each of the medical device's authentication interfaces mentioned in (1).
3) For brute-force prevention measures other than rate limiting policies, the manufacturer shall provide supporting evidence (e.g., screenshots of OTPs process, documentation, login validity period after OTP requested, etc.) demonstrating how the mechanism works.
4) For rate limiting policies, the manufacturer shall provide:
   a. The maximum number of attempts (the threshold) within a given period (or attempts per IP address) and the result of exceeding it (e.g., explain what happens after hitting the threshold – IP blocked, delay enforced, etc.).
   b. Supporting evidence (e.g., screenshots, documentation, videos, etc.) showing the rate limiting policy in effect (i.e., error messages from hitting the maximum login attempts, lockout period, etc.).
   c. A calculation using the provided formula (below) to demonstrate that the rate limiting policy meets the requirements specified above.

Estimated number of days required for a successful brute-force attack	$$\frac{\left(\left(\frac{C}{A}\right) \times [(A \times T) + L]\right)}{D}$$ Where: $C = (Number\ of\ possible\ characters)^{Password\ Length}$ $A = Number\ of\ attempts\ before\ lockout\ or\ threshold$ $L = Lockout\ period\ in\ seconds\ (e.g., 30s, 60s, 300s\ etc.)$ $T = Time\ for\ each\ attempt\ in\ seconds\ (e.g.,\ 0.5s, 1s, etc.)$ $D = Number\ of\ seconds\ in\ a\ day = 86400\ seconds$
Estimate % chance of success for a brute-force attack	$$\frac{Number\ of\ IP\ addresses\ \times Tries\ per\ IP\ address}{Number\ of\ possible\ characters^{(Password\ Length)}} \times 100\%$$

5) **Alternatively**, for medical devices without brute-force prevention mechanisms on all its authentication mechanisms, the following evidence shall be provided:
    a. The manufacturer shall provide an explanation of the authentication process, showing how physical presence is required.
    b. The manufacturer shall provide evidence (e.g., photos, device-related documentation, or test reports, etc.) to demonstrate that access to the medical device's physical ports is either disabled or effectively restricted.
    c. If USB ports are required, the manufacturer shall provide evidence showing that these ports prevent the use of HIDs and the medical device prevents unauthorised script execution (e.g., through application whitelisting or access control mechanisms).

Assessment

- The assessor shall check that the manufacturer has provided a complete list of all the device's authentication interfaces, along with its corresponding authentication mechanisms.

- For brute-force prevention measures other than rate limiting policies, the assessor shall examine the evidence and/or description provided by the manufacturer to determine that the brute-force prevention measure is adequate in increasing the resistance of the authentication interface(s) to brute-force attacks.

- For rate limiting policies, the assessor shall examine the following:

    - That the manufacturer has stated a threshold and the resulting action when the threshold is reached (e.g., enforcing a delay on the authentication interface, IP blocked, etc.).

    - That the supporting evidence provided by the manufacturer shows that there is a rate limiting policy in effect.

    - That the calculation provided by the manufacturer shows that the rate limiting policy complies with the stated requirements.

- For medical devices without brute-force prevention mechanisms on all its authentication interfaces, the assessor shall check and verify the following:

    - That authentication requires the user to be physically present.

    - That the physical ports on the medical device are either disabled or has restricted access.

    - When USB ports are required, the assessor shall check and verify that Human Interface Device (HID) connectivity is disabled and that the medical device possesses the capability to prevent the execution of unauthorised scripts.

ROADMAP FOR MEDICAL DEVICE LIFE CYCLE (RDMP)

RDMP.1

The manufacturer shall consider cybersecurity risks and vulnerabilities as part of their overall risk management process throughout the lifecycle of the medical device.

Note: This provision is taken to be fulfilled if the medical device has been listed by the Health Sciences Authority (HSA) in either the Class A Medical Device Database or in the Singapore Medical Device Register (SMDR).

Intent of the Provision

The intent of this security provision is to ensure that the manufacturer incorporates a risk management process to address cybersecurity risks and to verify the security of the medical device and the effectiveness of its security controls.

Minimum Requirements

- Manufacturers shall have a risk management plan that identifies, assesses, and implements mitigation measures for relevant cybersecurity risks and vulnerabilities. The plan shall also specify how the effectiveness of these mitigation measures is monitored.
- Testing shall be performed on the medical device to verify the security of the device and the effectiveness of its risk controls.

For more information on proper cybersecurity risk management processes, refer to the following documents:

- **ISO 14971:2019** - Medical devices — Application of risk management to medical devices [4]
- **AAMI TIR57:2016/(R) 2019 -** Principles for medical device security-Risk management [5]

Supporting Evidence

1) The manufacturer shall provide their risk management plan.
2) The manufacturer shall provide evidence demonstrating that the security controls have been verified. Examples of acceptable evidence include:
    a. Description of test methodology, test results, and conclusions.
    b. A traceability matrix mapping security risks to security controls and the tests verifying those controls.
    c. References to any standards, internal SOPs, or documentation used during the process.

Assessment

- The assessor shall examine the evidence to determine that the manufacturer's risk management plan includes:
  - The identification, assessment, and mitigation of relevant cybersecurity risks or vulnerabilities.
  - The monitoring of the effectiveness of implemented mitigation measures.

- The assessor shall examine the test reports or documentation to determine that the security of the device and the effectiveness of its security controls have been validated.

RDMP.2

The manufacturer shall follow a secure software development process during product development and evaluate third-party applications and software components included in the medical device as part of secure development practices.

Intent of the Provision

The intent of this provision is to ensure that the manufacturer adopts secure software development lifecycle (SDLC) processes during product development and establishes a process to evaluate third-party applications and software components before their integration into the medical device.

Minimum Requirements

- The manufacturer shall implement SDLC processes, adopting at least one activity from each of the following categories. Alternative activities related to these categories may also be proposed:
  - Software Development Planning
    - Utilisation of a Software Configuration Management (SCM) tool.
    - Ensuring the security of the development environment.
    - Incorporating Secure by Design principles into the software development process.
  - Software Requirements Analysis
    - Conducting risk analysis and threat modelling.
    - Identifying and documenting security objectives and requirements.
    - Reviewing security requirements to ensure that risks and threats are managed and addressed.
  - Software Architectural Design
    - Developing a secure architecture that implements security policies (e.g., access control, data protection, authentication, security enforcement, etc.).
    - Incorporating secure design best practices (i.e., principle of least privilege, trust boundaries, attack surface reduction, security roles/privileges and access control, secure by default principle).
    - Using secure best practice cryptographic protocols and algorithms.
  - Implementation
    - Enforcing use of secure coding standards.
    - Conducting peer code review.
    - Conducting code analysis (static/dynamic).
  - Evaluation of Third-Party Applications and Software Components
    - Implementing an evaluation process to assess third-party applications and software components for its security.
      - Assessing track record of third-party applications and software components, including known vulnerabilities and security incidents
      - Ensuring that security controls implemented by third-party vendors for these components are adequate for the device.
    - Conducting software composition analysis.

- Functional Testing
  - Conducting unit and integration tests.
- Security Testing
  - Performing threat mitigative testing.
  - Performing vulnerability testing, including malformed or unexpected input testing, and the use of vulnerability scanning tools.
  - Conducting penetration tests.

For more information on secure software development lifecycle processes, refer to the following documents:

- ISO/IEC 81001-5-1 “Health informatics – Management and governance of health software systems – Part 5-1: Health software system safety, security and performance” [6]
- U.S. Food and Drug Administration – FDA-2021-D-1158 - “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions” [7]
- EU MDCG 2019-16 Rev.1 “Guidance on Cybersecurity for medical devices” [8]
- ISO/IEC 27034-1:2011 “Information Security – Security Techniques – Application security Part 1: Overview and concepts” [9]
- IEC 62304:2006 “Medical device software – Software life cycle processes” [10]
- ISO 13485:2016 “Medical devices – Quality management systems – Requirements for regulatory purposes” [11]

Supporting Evidence

1) The manufacturer shall state if any SDLC publications have been referenced or adopted.

2) The manufacturer shall provide evidence (e.g., process or guidance documents, device whitepapers, test reports, etc.) to show that secure SDLC processes have been followed in the medical device’s development.

Assessment

- The assessor shall examine the evidence to determine that the manufacturer has adopted SDLC processes.

RDMP.3

The manufacturer shall maintain a webpage (or use other avenues) to provide information on the medical device's software support period and updates.

Intent of the Provision

The intent of this provision is to ensure that the manufacturer offers a reliable method for device owner/operators to access information regarding the medical device's software support period and updates.

Minimum Requirements

- The device manufacturer shall maintain an avenue (e.g., webpage or other avenues) for disseminating information regarding the medical device's software support period and updates. This avenue may be accessible to the public or exclusively to customers.

- The software support period shall be clearly indicated, including a specific date (day, month, and year) until which the manufacturer guarantees support for the medical device.

Supporting Evidence

1) The manufacturer shall provide details of the avenues used to share information and provide evidence (e.g., screenshots, webpage URLs, etc.) demonstrating how medical device owners/operators can access the information.

Assessment

- The assessor shall check and verify that there is an avenue maintained by the manufacturer that provides information regarding software support period and updates.

- The assessor shall check and verify that the software support period is clearly specified.

RDMP.4

The manufacturer shall have a plan in place for managing the end-of-life (EOL) and end-of-support (EOS) of third-party components.

Intent of the Provision

The intent of this provision is to ensure that the manufacturer has a process to manage third-party components as they reach EOL or EOS. This ensures that third-party components are monitored, and appropriate actions or measures are taken when they reach EOL or EOS.

Minimum Requirements

- The manufacturer shall have processes in place to manage the EOL or EOS of third-party components, including the following steps:
    - Maintaining an inventory of all third-party components and dependencies used in the device *(Note: this can be achieved by fulfilling requirements of SBOM.1).*
    - Regularly assessing the EOL/EOS status of third-party components to identify potential risks, either through communication with vendors or by other means.
    - Conducting Risk Assessments to ascertain the potential impact of EOL/EOS components on the security of the device.
    - Mitigation Planning to address potential impact caused by components reaching EOL/EOS, including identifying alternatives, seeking extended support options, or even planning for upgrades/replacements.
    - Ensuring Security Updates and Patches for EOL/EOS third-party components to mitigate known vulnerabilities and reduce risk of exploitation.
    - Testing and Validation to ensure that device security is maintained after updates/patches or after the implementation of mitigation to address EOL/EOS components.
    - Documentation to ensure that all actions taken to address EOL/EOS are recorded.

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., process documents, post-market strategy plans, etc.) demonstrating the plan for managing third-party component EOL or EOS.

Assessment

- The assessor shall examine the evidence to determine that the manufacturer's processes include the steps outlined in the minimum requirements.

SOFTWARE BILL OF MATERIALS (SBOM)

SBOM.1

The manufacturer shall provide a Software Bill of Materials (SBOM) for the medical device's firmware, related applications (e.g., desktop or mobile applications such as iOS and Android), and any other applicable software components.

Intent of the Provision

The intent of this provision is to ensure that the manufacturer maintains an SBOM for the medical device to facilitate the monitoring of components and its associated vulnerabilities. The SBOM helps in deploying targeted updates and remediation measure to maintain the safety and essential functionality of the device.

Minimum Requirements

- The SBOM shall include all software and firmware components used by the medical device, including third-party software, libraries, and operating systems.

- The SBOM shall be presented as:
  - A single, comprehensive SBOM covering the product's software, firmware, and other related applications, **or**
  - Individual SBOMs for the product's software, firmware, and each of the other related applications.

- The following details shall be present in the SBOM(s):
  - Component Name
  - Component Version (e.g., version numbers, version identifiers)

Supporting Evidence

1) The manufacturer shall provide the latest SBOM(s) that encompass all the software, firmware, and other related applications (i.e., underlying OS, mobile applications, etc.) components used by the medical device.

   NOTE: Manufacturers may include SOUPs (Software of Unknown Provenance) as supplementary information in their SBOM submissions; however, SOUPs cannot serve as a substitute for a complete SBOM submission.

Assessment

- The assessor shall check the SBOM(s) to verify that it contains the details specified in the minimum requirements.

SYSTEM AND APPLICATION HARDENING (SAHD)

SAHD.1

The manufacturer shall harden the medical device in accordance with industry standards.

Intent of the Provision

The intent of this provision is to ensure that the manufacturer has implemented appropriate security hardening measures for the medical device.

Minimum Requirements

- The manufacturer shall implement measures to harden the medical device. Examples of such measures include, but are not limited to:
    - Hardening the medical device in accordance with industry standards and best practices.
    - Implementing other forms of security hardening to address specific attack vectors, even if not explicitly mentioned in industry standards and best practices.

Possible examples of industry standards and best practices include, but are not limited to:

- International Medical Device Regulators Forum Medical Device Cybersecurity Guide
- FDA Guidance
- EU Medical Device Coordination Group Guidance
- National Institute of Standards and Technology (NIST) guidelines
- OWASP Guidelines

Possible examples of security hardening for addressing specific attack vectors are, but not limited to the following:

Security Hardening Measure:	**Attack Vector Addressed:**
Access Control and Authentication	- Brute-force attacks - Unauthorised access
Regular Software Updates and Patching	- Known vulnerabilities - Firmware exploits
Secure Boot and Code Signing	- Firmware/software tampering - Malware injection

Supporting Evidence

1) The manufacturer shall provide details of the industry standard(s) used for hardening the medical device, or evidence (e.g., screenshots, device documentation) showing the implementation of security hardening measures.

Assessment

- The assessor shall check that the manufacturer has referenced any industry standards, or examine the evidence provided by the manufacturer to verify if there are security hardening measures implemented on the medical device.

SAHD.2

The medical device shall employ mechanism for software integrity checking.

Intent of the Provision

The intent of this provision is to ensure that the medical device implements at least one mechanism for software integrity checking.

Minimum Requirements

- The device shall use at least one of the following mechanisms for software integrity checking by employing best practice cryptography (refer to NIST SP 800-131A [3] or NIST SP 800-52 [2]):
    - Hash Verification
    - Digital Signatures
    - Secure Boot
    - File Integrity Monitoring

Supporting Evidence

1) The manufacturer shall specify the software integrity checking mechanism(s) used, including the cryptographic algorithms employed.
2) The manufacturer shall provide evidence (e.g., device whitepapers, device information documents, etc.) demonstrating that the software integrity checking mechanism(s) mentioned in (1) is implemented on the medical device.

Assessment

- The assessor shall check that the device has software integrity checking capabilities implemented on the medical device.

SAHD.3

All unnecessary resources and services (i.e., file shares, COTS applications, etc.) which are not required shall be disabled or removed.

Intent of the Provision

The intent of this provision is to ensure that manufacturers have processes in place as part the secure-by-design principle to disable or remove all unnecessary resources and services on the medical device to reduce its overall attack surface.

Minimum Requirements

- The manufacturer shall have a process in place as part of the secure-by-design principle to disable or remove unnecessary resources and services on the medical device.

Examples of resources and services that are commonly present on medical devices that may be unnecessary for its purpose include, but are not limited to:

- Unnecessary Network Services (e.g., file sharing, media sharing, remote access, Telnet, etc.).
- Non-Essential Consumer Applications (e.g., non-medical productivity software, entertain apps, games, etc.).
- Unused or redundant software.

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., Product lifecycle documentation, vulnerability assessment reports, configuration management plan, system hardening checklists, etc.) to demonstrate that a process exists to disable or remove unnecessary resources and services of the medical device.

Assessment

- The assessor shall examine the evidence provided by the manufacturer to determine that a process is in place to disable or remove unnecessary resources and services on the medical device.

SAHD.4

The manufacturer shall disable all network communication ports and protocols that are not required by default.

Intent of the Provision

The intent of this provision is to ensure that all unused or unnecessary communication ports and protocols on the medical device are disabled to minimise its overall attack surface.

Minimum Requirements

- All network communication ports and protocols that are not required for the medical device's operation shall be disabled.

For reference, this is a non-exhaustive list of the common communication ports and protocols in medical devices:

- TCP/IP ports
  - Domain Name System (DNS), 53
  - Hypertext Transfer Protocol (HTTP), 80
  - Hypertext Transfer Protocol Secure (HTTPS), 443
  - File Transfer Protocol (FTP), 21
  - Secure Shell (SSH), 22
  - Simple Mail Transfer Protocol (SMTP), 25
- UDP ports
  - Syslog, 514
- Digital Imaging and Communications in Medicine (DICOM), 104
- DICOMweb, 80 or 443
- Health Level 7 (HL7), 2575
- Medical Device Data Systems (MDDS), 8080
- RS-232
- USB Serial
- Universal Asynchronous Receiver-Transmitter (UART)
- Inter-process communication mechanisms
- Application programming interfaces (APIs)

Supporting Evidence

1) The manufacturer shall provide a list of all network communication ports and protocols enabled by default on the medical device, along with a rationale for their necessity.

2) The manufacturer shall provide the output (e.g., screenshots, etc.) of an NMAP scan that identifies all open TCP and UDP ports on the device, including both the LAN and WAN interfaces, where applicable.

   a. The NMAP scan shall be performed using the command: *nmap -sT -sU -A -p -<IP Address>*

Assessment

- The assessor shall check the list of enabled network communication ports and protocols to verify that there is a reasonable rationale justifying each enabled port/protocol.

- The assessor shall check the NMAP scan output to verify that all enabled ports and protocols on the device are accounted for.

SECURITY GUIDANCE (SGUD)

SGUD.1

The manufacturer shall provide security documentation for the medical device owner/operator.

Intent of the Provision

The intent of this security provision is to ensure that the security documentation provided to the medical device owners/operators includes guidance on how to configure and operate the device securely.

Minimum Requirements

- The security documentation (i.e., user guidance documents, device setup guide, etc.) provided to medical device owners/operators shall include guidance/instructions on how to securely set up, configure and operate the medical device.

Examples of guidance that can be included in the security documentation are, but not limited to:

- How to set up multi-factor authentication (if supported by the medical device).
- Guidance to configure access control mechanisms.
- Managing user account and roles.
- Network access control configuration.

The security documentation may be part of the medical device's installation or configuration guide.

Supporting Evidence

1) The manufacturer shall provide the security documentation (e.g., user guidance documents, device setup guide, etc.) that is provided to medical device owners/operators.

2) For devices set up by the manufacturer’s representatives (e.g., field service engineer, etc.), the manufacturer shall also provide the documentation used by their representative during the set up or configuration process.

Assessment

- The assessor shall examine the security documentation to determine that sufficient guidance is provided to medical devices/operators to securely configure and operate it.

SGUD.2

The medical device shall have the capability to permanently delete of sensitive or PII data from the device or media. The manufacturers shall provide the necessary instructions for the feature.

Intent of the Provision

The intent of this provision is to ensure that medical device owners/operators can permanently delete sensitive or PII data from the device for the purposes of decommissioning or redeployment.

Minimum Requirements

- For all data listed in MSD.1, the medical device shall have at least one feature (e.g., through the GUI, through the companion mobile application, using the hardware reset function, etc.) that allows owners/operators to permanently delete this data.

- Information on the existence of these features and instruction on how to use them shall be provided to medical device owners/operators.

Supporting Evidence

1) The manufacturer shall list all features that enable the permanent deletion of sensitive or PII data on the medical device or media.

2) The manufacturer shall provide evidence (e.g., user guidance documents, screenshots, URLs, etc.) demonstrating the existence of these features and instructions on how to use them.

Assessment

- The assessor shall check and verify that the medical device has at least one feature allowing owners/operators to permanently delete sensitive or PII data from the device or media.

- The assessor shall check the evidence to verify that usage instructions are available to medical device owners/operators.

SGUD.3

The manufacturer shall document all pre-installed user accounts on the medical device, including default accounts such as technician, service, administrator, etc., and provide this information to the device owner/operator.

Intent of the Provision

The intent of this provision is to ensure that the manufacturer provides device owners/operators with information about pre-installed accounts on the medical device, enabling them to assess potential security risks associated with these accounts.

Minimum Requirements

- The manufacturer shall provide medical device owners/operators with information regarding all pre-installed user accounts, including technician, service, and administrator accounts.

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., device documentation, emails, webpages, etc.) demonstrating that device owners/operators are provided with information on all pre-installed user accounts.

2) The manufacturer shall provide evidence (e.g., device documentation, emails, webpages, etc.) demonstrating that information on all pre-installed user account is made available to medical device owners/operators.

Assessment

- The assessor shall check the evidence to verify that information on pre-installed user accounts is made available to medical device owners/operators.

HEALTH DATA STORAGE CONFIDENTIALITY (STCF)

STCF.1

The medical device shall support encryption of sensitive data at rest.

Intent of the Provision

The intent of this provision is to ensure that all sensitive data stored on the medical device is encrypted while at rest.

Minimum Requirements

- The medical device shall have the capability to encrypt sensitive data at rest.
- Best practice cryptography shall be used, following standards such as NIST SP 800-52 [2] or NIST SP 800-131A [3].

Examples of encryption methods/mechanisms include, but are not limited to:

- Full disk encryption (e.g., Bitlocker, FileVault, VeraCrypt, LUKS, etc.)
- File-level encryption (e.g., Microsoft EFS, GNU Privacy Guard, etc.)
- Database encryption (e.g., Transparent Data Encryption (TDE), column-level encryption, etc.)
- Cloud-based encryption (Amazon Key Management Service, Microsoft Azure Key Vault, Google Cloud Key Management Service, etc.)
- Application-level encryption (e.g., application implements encryption functionalities and performs encryption on sensitive data at rest, etc.)

Supporting Evidence

1) For all sensitive data listed in MSD.1, the manufacturer shall provide:
    a. Location of the data (e.g., stored in hard disk, database server, cloud, removable storage, etc.).
    b. Encryption method used or mechanism used to encrypt the data.
    c. Cryptographic algorithm, key size(s), referenced standards and unique identifier of the encryption key.

Assessment

- The assessor shall examine the evidence to determine that the encryption method or mechanism used for sensitive data at rest is adequate and follows best practice cryptography.

TRANSMISSION CONFIDENTIALITY (TXCF)

TXCF.1

The medical device shall encrypt sensitive data prior to transmission via a network or removable media by default.

Intent of the Provision

The intent of this provision is to ensure that sensitive data is protected using best practice cryptography before it is transmitted over a network or through removable media.

Minimum Requirements

- The medical device must have the capability to encrypt sensitive data using best practice cryptography before transmission via a network or removable media.

Acceptable examples include, but are not limited to:

- Communication (e.g., transmission channel, etc.) between the device and a network shall be established using TLS 1.2 or higher, with acceptable cipher suites (refer to NIST SP 800-52 [2]).
- For Wi-Fi communications, WPA2 or higher communication protocol shall be implemented while conforming to the best cryptographic practices for encryption algorithm as per NIST SP 800-131A [3].
- For Bluetooth communication (including BLE), it shall be configured as Security Mode 1 with Security Level 3 minimally (but excluding Security Mode 2 with Security level 1).
- Digital Imaging and Communication in Medicine (DICOM).
- Health Level 7 (HL7).
- IEEE 11073 Standards Family for Health Informatics.
- File encryption.

Supporting Evidence

1) For all data listed in MSD.1, the manufacturer shall provide a list of all communicating entities (e.g., devices, services, networks, etc.) between which sensitive data is transmitted.

   Possible examples of such communication include, but are not limited to:

   - Device to another medical device.
   - Device to mobile application (companion app).
   - Device to web/cloud services.
   - Device to Laboratory Information Systems/LDAP.
   - Device's wireless/wired connection functionalities (e.g., Wi-Fi, Bluetooth, etc.).
   - Exporting of sensitive or PII data to removable media.

2) For each communication listed, the manufacturer shall provide evidence demonstrating that sensitive data is encrypted before transmission. This shall include:
    a. The encryption method used or mechanism used to encrypt the data.
    b. Cryptographic algorithm and key sizes, referenced standards, and unique identifier of the key.
    c. Evidence (e.g., screenshots, device documentation, etc.) demonstrating that the communication is secure between the entities.
        i. For TLS Implementations, refer to **Annex A** for more information.

Assessment

- The assessor shall check and verify that all communicating entities (e.g., devices, services, networks, etc.) where sensitive or PII data is transmitted are accounted for.
- For each communication stated by the manufacturer, the assessor shall check and verify that the sensitive data is encrypted prior to transmission.
- The assessor shall examine the evidence to determine that sensitive data is encrypted using best practice cryptography prior to transmission and that the implementation adequately protects the confidentiality of the data.
    - The assessor may enhance the assessment by leveraging insights gained from the assessment of other security provisions and supporting evidence outlined in this document for the assessment of the completeness of the list of communicating entities.

TRANSMISSION INTEGRITY (TXIG)

TXIG.1

The medical device shall support mechanisms (i.e., digital signatures, hash-based message authentication code) to ensure that data is not modified during transmission.

Intent of the Provision

The intent of this provision is to ensure that data remains unmodified during transmission by utilising best practice cryptography.

Minimum Requirements

- The medical device shall have the capability to prevent data modification during transmission by using best practice cryptography to ensure data integrity.

Examples of how data integrity during transmission can be ensured include, but are not limited to:

- Transport Layer Security (TLS) 1.2 or higher, with acceptable cipher suites (refer to NIST SP 800-52 [2])
- Hash-based message authentication code (HMAC)

Supporting Evidence

1) The manufacturer shall provide a list of all communicating entities (e.g., devices, services, networks, etc.) involved in data transmission.

   Possible examples of such communication include, but are not limited to:

   - Device to another medical device.
   - Device to mobile application (companion app).
   - Device to web/cloud services.
   - Device to Laboratory Information Systems/LDAP.
   - Device's wireless/wired connection functionalities (e.g., Wi-Fi, Bluetooth, etc.).
   - Exporting of sensitive or PII data to removable media.

2) For each of the communications listed, the manufacturer shall provide evidence to showing how data integrity is ensured. The evidence shall include:

   - The protocol (e.g., TLS, etc.) or algorithm (e.g., HMAC, etc.) used to ensure data integrity.
   - The cryptographic algorithm and key sizes, referenced standards, and unique identifier of the encryption key.

Assessment

- The assessor shall examine the evidence to determine that all communicating entities are accounted for and that data integrity is maintained between each entity during transmission.

REMOTE SERVICE (RMOT)

RMOT.1

The medical device shall indicate when there is an active or enabled remote session.

Intent of the Provision

The intent of this provision is to ensure that the medical device can notify or alert the owner/operator when there is an incoming request for a remote session and when a remote session is active. This aids owners/operators in identifying potential unauthorised or suspicious remote session activities.

Minimum Requirements

- The medical device shall have the capability to inform device owners/operators when there is an incoming request for a remote session.
- The medical device shall have the capability to inform device owners/operators if there are any ongoing remote sessions.

Examples of how the medical device can indicate remote session include, but are not limited to:

- Session tracking mechanism to monitor and track local and remote active user sessions.
- Remote session identification.
- Real-time alerts to notify administrators or users when a remote session is initiated or terminated.

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., device whitepapers, screenshots, or videos of how a remote session is initiated on the device, etc.) demonstrating that the medical device can indicate when an incoming request for a remote session is received, as well as when remote sessions are active.

2) The manufacturer shall provide evidence (e.g., device whitepapers, screenshots, or videos of alerts/indicators during an active remote session, etc.) showing alerts or indicators during an active remote session.

Assessment

- The assessor shall check the evidence to verify that the medical device can indicate when an incoming remote session request is received.
- The assessor shall check the evidence to verify that the medical device can indicate when a remote session is active.

OTHER SECURITY CONSIDERATIONS (OTHR)

OTHR.1

The manufacturer shall ensure, through technical or procedural means, that the remote user performing remote administration on the medical device is authenticated and legitimate.

Intent of the Provision

The intent of this provision is to ensure that the remote user performing administrative tasks on the medical device can be authenticated and verified to be legitimate.

Minimum Requirements

- The medical device shall require the use of technical means to perform authentication before initiating a remote administration session.

Possible examples of authentication methods include, but are not limited to:

- Two-Factor Authentication (2FA).
- Multi-Factor Authentication (MFA).
- Dual-login (i.e., the “four-eyes” principle, where both the remote and local users must approve the session request).

- **Alternatively**, the manufacturer may define procedural methods to verify the identity of the remote administrative user.

Possible examples of procedural verification methods include, but are not limited to:

- Phone or video calls to verify the legitimacy of all participants (e.g., remote user, local user, support representative, etc.).

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., screenshots, documentation, etc.) that outlines the usage instruction for the technical or procedural methods used to authenticate or verify the identity of the remote administrative user.

Assessment

- The assessor shall examine the evidence to determine that the technical or procedural methods used for authentication are sufficient to guarantee the authenticity and legitimacy of the remote user performing administrative tasks on the medical device.

OTHR.2

The medical device shall employ recommended industry standard Wi-Fi security protocols (i.e., WPA2/3, etc.).

Intent of the Provision

The intent of this provision is to ensure that the medical device uses appropriate and recommended security protocols for Wi-Fi, such as WPA2 or WPA3 (if supported).

Minimum Requirements

- The medical device shall use appropriate and recommended security protocols for Wi-Fi (i.e., WPA2, or WPA3 if supported) and have them enabled by default.

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., screenshots of GUI, device documentation, output of Wi-Fi analyser tools, etc.) showing the Wi-Fi security protocols supported by the medical device.

2) The manufacturer shall confirm that the Wi-Fi security protocols supported by the device are enabled by default.

Assessment

- The assessor shall check and verify that the device uses the appropriate and recommended Wi-Fi security protocols and verify that they are enabled by default.

OTHR.3

If not required, local interfaces (i.e., USB, SD card readers) that support the use of removable storage media on the medical device shall be logically and/or physically disabled by default (e.g., tamper-evidence stickers, port blockers, etc.).

Intent of the Provision

The intent of this provision is to ensure that unused local interfaces are logically or physically disabled to minimise the medical device's attack surface.

Minimum Requirements

- All unused local interfaces shall be disabled, either through logical or physical means.

Supporting Evidence

1) For local interface(s) that are not required by the medical device, the manufacturer shall provide evidence (e.g., screenshots, device documentation, pictures, videos, etc.) demonstrating that they have been disabled either logically or physically.

Assessment

- The assessor shall examine the evidence to determine that sufficient measures have been taken to disable local interfaces that are not required by the device.

REFERENCES

[1] International Organization for Standards, International Electrotechnical Commission, ISO/IEC 29147:2018(E), Information technology - Security techniques - Vulnerability disclosure.

[2] National Institute of Standards and Technology, NIST SP 800-52 Revision 2, Guidelines for the Selection, Configurationi, and use of Transport Layer Security (TLS) Implementations.

[3] National Institute of Standards and Technology, NIST SP 800-131A Revision 2, Transitioning the Use of Cryptographic Algorithms and Key Lengths.

[4] International Organization for Standards, ISO 14971:2019, Medical devices - Application of risk management to medical devices.

[5] Association for the Advancement of Medical Instrumentation [AAMI], AAMI TIR57:2016/(R) 2019 - Principles for medical device security - Risk management.

[6] International Organization for Standards, International Electrotechnical Commission, ISO/IEC 81001-5-1, Health informatics - Management and governance of health software systems - Part 5-1: Health software system safety, security and performance.

[7] U.S. Food & Drug Administration, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions.

[8] Medical Device Coordination Group, MDCG 2019-16 Rev.1 Guidance on Cybersecurity for medical devices.

[9] International Organization for Standards, International Electrotechnical Commission, ISO/IEC 27034-1:2011, Information Technology - Security techniques - Application security - Part 1: Overview and concepts.

[10] International Electrotechnical Commission, IEC 62304:2006, Medical device software - Software life cycle processes.

[11] International Organization for Standards, ISO 13485:2016, Medical devices - Quality management systems - Requirements for regulatory purposes.

ANNEX A – SUPPORTING EVIDENCE FOR TLS

In cases where TLS is used for secure communication, the manufacturer shall identify whether the medical device functions as the client or the server in the TLS connection.

If the medical device functions as the client, the manufacturer shall provide a Wireshark screenshot showing the following information:

1) Source and destination IP address
2) Open a "Client Hello" packet from this specific source and destination IP address to show the following (as indicated in reference image below):
    a. TLS version
    b. Cipher Suites

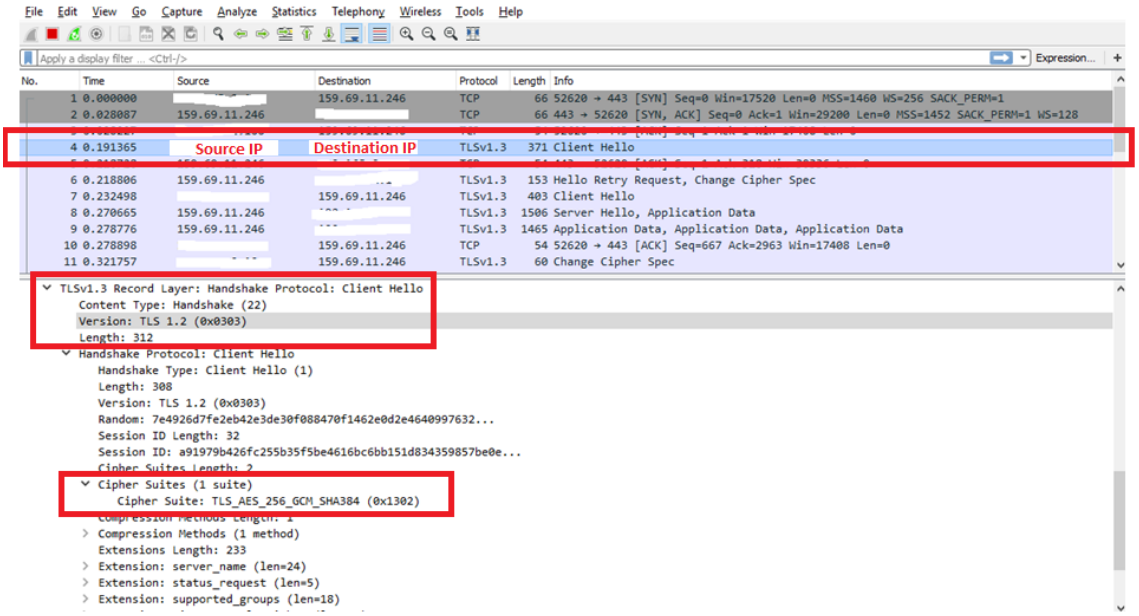

Image 1 – Highlighted information that should be included in the Wireshark screenshot

If the medical device functions as the server, the manufacturer shall provide a screenshot of the testssl.sh output showing supported cipher suites. Refer to image below.

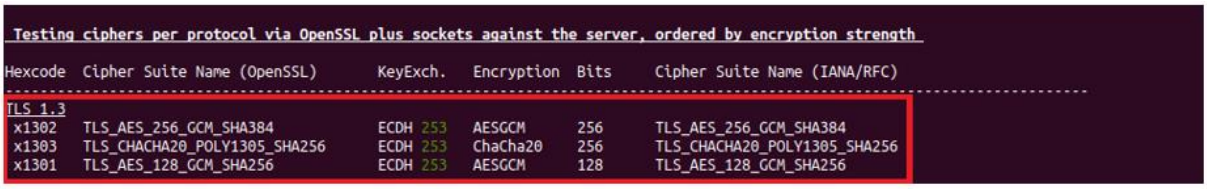

Image 2 – Highlighted information that should be included in the testssl.sh screenshot

For medical devices that use publicly accessible authentication servers (e.g., Identify Providers, Authentication APIs, etc.) for user authentication an SSL Server Testing Tool may be used to provide supporting evidence.

The manufacturer shall provide the following:

1) URL to the publicly accessible authentication server.
2) Use the SSL Server Testing Tool to generate an SSL report and save it in PDF format. This can be obtained by selecting to print the page from the browser and choosing to save it as PDF.