Cybersecurity Labelling Scheme

FOR MEDICAL DEVICES

BY CYBER SECURITY AGENCY OF SINGAPORE

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

Assessment Methodology

April 2024
Version 0.4

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

CONTENTS

INTRODUCTION

This document specifies the assessment methodology for 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:

- **Status** – Indicates the status of a provision.
- **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.
    - "Examine" – Assessor will generate a verdict by performing 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

TERMS AND DEFINITIONS

Term	Definition
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.
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 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.
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.
Constrained Devices	RFC 7228: Small devices with limited CPU, memory, and power resources.

	Constrained node: A node where some of the characteristics that are otherwise pretty much taken for granted for Internet nodes at the time of writing are not attainable, often due to cost constraints and/or physical constraints on characteristics such as size, weight, and available power and energy. The tight limits on power, memory, and processing resources lead to hard upper bounds on state, code space, and processing cycles, making optimization of energy and network bandwidth usage a dominating consideration in all design requirements. Also, some layer services such as full connectivity and broadcast/multicast may be lacking. Although constrained devices are exempted to meet certain provisions, it is strongly recommended that constrained devices should still try to meet the requirement to ensure higher security.
Update Mechanisms	Ways that a medical device can receive and install firmware updates. Examples: Automatic update and manual update feature found on the device.
Simple-to-use	Feature on the device that users can interact with, without requiring prior technical knowledge. Example: Installing updates through the push of a button, automatic updates, not requiring CLI usage to initiate device updates, erasing personal data from the device from a push of a button, 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.
MAB	MAC Authentication Bypass is an access control protocol that allows access using a machine's MAC address (Media Access Control Address).
802.1X	It is a network authentication protocol that opens ports for network access when a user's identity is authenticated and authorizes for access to the network.
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
CLI	Command Line Interface
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
MAB	MAC Authentication Bypass
MFA	Mult-Factor Authentication
PII	Personal Identifiable Information
CPE	Common Platform Enumeration
PURL	Package URL
UUID	Universal Unique Identifier
GUID	Globally Unique Identifier
SWHID	Software Heritage ID
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.

Status

The provision is **mandatory**.

This provision is taken to be fulfilled if the 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 there is a mechanism for device owners/operators to report vulnerabilities to the manufacturers and that there are processes in place to communicate vulnerabilities and remediating actions 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 on the device.
    - Propose remediating actions to affected stakeholders.

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., contact information, support emails, support hotlines, etc.) to demonstrate the mechanism that device owners/operators use to contact the manufacturer to report vulnerabilities.

2) The manufacturer shall describe the processes in place to:
    - Gather information from vulnerability finders.
    - Disclose the existence of vulnerabilities on the device.
    - Propose remediating actions to affected stakeholders.

Assessment

- The assessor shall check that there is a way for device owners/operators to contact the manufacturer to report vulnerabilities.

- The assessor shall check that there are processes in place to gather information from vulnerability finders, disclose the existence of vulnerabilities and propose remediating actions to affected stakeholders.

VDP.2

The manufacturer shall provide a vulnerability disclosure policy (i.e., ISO/IEC 29147, etc.) covering the device.

Status

The provision is **mandatory**.

Intent of the Provision

The intent of this provision is to ensure that there is a vulnerability disclosure policy (VDP) covering the device.

Minimum Requirements

- The VDP covering the device shall be publicly available and accessible. This can be achieved by making the VDP available on the manufacturer's website, or by utilising a bug bounty platform.
- The VDP shall contain the following essential components:
  - Contact information for reporting of vulnerabilities.
  - Clear instructions on how vulnerabilities can be reported.
  - Outlining expectations in timeline for the initial acknowledgement of receipt (e.g., within 7 working days, etc.) and status updates until the resolution of vulnerability.

Guidelines on VDPs are available at:

- ISO/IEC 29147:2018: "Information technology – Security Techniques – Vulnerability Disclosure"
- OASIS: "CSAF Common Vulnerability Reporting Framework (CVRF)"
- OWASP: "Vulnerability Disclosure Cheat Sheet"

Supporting Evidence

1) The manufacturer shall provide the weblink and PDF print of the VDP or bug bounty platform covering the device.

Assessment

- The assessor shall check that the manufacturer uses either a VDP or a bug bounty platform to cover the device.
- The assessor shall check that the manufacturer's VDP or bug bounty platform is publicly available and accessible.
- The assessor shall examine the VDP webpage or bug bounty platform to determine that it contains the essential components mentioned in the minimum requirements above.

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 device.

Status

The provision is **mandatory**.

Intent of the Provision

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

Minimum Requirements

- There shall be a maintained list of all sensitive data that is either collect by the device or transmitted/transferred by the device.
- 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 device.
    a. Where applicable, the manufacturer shall clearly state what sensitive data is being transmitted/transferred and where it is being sent (e.g., backed up to a database, stored on remote server, removable storage, etc.).
2) For each sensitive data listed in (1), the manufacturer shall provide the rationale for the necessity on its the collection and transmission.
3) If the device does not collect or transmit/transfer sensitive data, the manufacturer shall provide a statement confirming this.

Assessment

- The assessor shall examine the list and rationale to determine that all sensitive data collected or transmitted by the device are necessary.

AUDIT CONTROLS (AUDT)

AUDT.1

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

Status

The provision is **mandatory for unconstrained devices.**

Intent of the Provision

The intent of this security provision is to ensure that logs or reports created by the device for the purpose of facilitating investigations, audit, and even forensic analysis in the event of cybersecurity incidents, do not include sensitive data in clear text.

Minimum Requirements

- The device shall have the capability to capture and store device logs or audit trails.
- The device shall not store sensitive information in clear text in all device logs and audit trails.

Supporting Evidence

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

Assessment

- The assessor shall check that the device is able to capture and store device logs or audit trails.
- The assessor shall examine the logs or audit trails provided to determine that it does not contain sensitive data.

AUDT.2

The device shall be able to log actions and activities performed on the device.

Status

The provision is **mandatory for unconstrained devices.**

Intent of the Provision

The intent of this security provision is to ensure that security relevant actions and activities are logged to facilitate investigation, audit, and forensic analysis in the event of a cybersecurity incident.

Minimum Requirements

- The device shall have the capability to capture security relevant actions and activities to facilitate investigation, audit, and forensic analysis.

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

- 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 list of all security-relevant actions and activities that are logged in either the device logs or audit trails.

Assessment

- The assessor shall check the device logs or audit trails provided to determine that the device captures security relevant actions and activities listed by the manufacturer.

AUTHORISATION (AUTH)

AUTH.1

Access to the device's functionalities and resources shall be restricted to authorised users, ensuring that individuals can only access what is permitted to them.

Status

The provision is **mandatory.**

Intent of the Provision

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

Minimum Requirements

- After authentication, the device shall have the capability to restrict access to the device's functionalities and resources based on what the user is permitted to.
- The device shall only have pre-installed privileged users and roles (e.g., Administrator, Guest/Demo, Technical Support, Service accounts, etc.) which are required.

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., screenshots, device documentation, etc.) demonstrating the device's capability to restrict access to its functionalities and resources based on the user's defined permissions.
2) The manufacturer shall provide a list of users and roles that are pre-installed onto the device and provide a rationale for its necessity.

Assessment

- The assessor shall examine the evidence to determine that the device has the capability to restrict access to the device's functionalities and resources based on what the user is permitted to.
- The assessor shall examine the list and the corresponding rationale to determine that the pre-installed users and roles are necessary.

AUTH.2

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

Status

The provision is **mandatory for unconstrained devices.**

Intent of the Provision

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

Minimum Requirements

- The device shall have the capability to support access control mechanisms (e.g., defining roles, creation of user groups, setting of rule-based policies, etc.).

- The device shall have the capability to allow 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 device supports access control mechanisms.

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

Assessment

- The assessor shall examine the evidence to determine that the device supports access control mechanisms.

- The assessor shall examine the evidence to determine that the device supports the management and assignment of roles and privileges to other users by authorised users.

CYBER SECURITY PRODUCT UPGRADES (CSUP)

CSUP.1

Manufacturer shall have an on-going plan to remediate cybersecurity vulnerabilities to ensure device performance and safety is not compromised throughout the device's lifecycle.

Status

The provision is **mandatory**.

This provision is taken to be fulfilled if the 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 remediate cybersecurity vulnerabilities to ensure device performance and safety is not compromised.

Minimum Requirements

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

Supporting Evidence

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

Assessment

- The assessor shall examine the supporting evidence provided to determine that the manufacturer has a plan to address vulnerabilities. The assessor shall examine the evidence to determine that the manufacturer has a plan to address vulnerabilities.

CSUP.2

Manufacturers shall have a process to notify and guide the device owner/operator to achieve a successful software update through instruction manuals and procedures on installation.

Status

The provision is **mandatory**.

Intent of the Provision

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

Minimum Requirements

- The manufacturer shall have a process or procedure to notify device owners/operators on the availability of a software update.
- For scenarios where the installation of software updates is carried out by the manufacturer's representatives (e.g., field support engineers, etc.), there shall be a standardised process and procedure for them to follow.
- These software update guidance/process/procedures shall be clear and easily understandable to facilitate the proper installation of software 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 device owners/operators are notified when a new software update is available.
2) The manufacturer shall provide the software update guidance (e.g., instruction manuals, etc.) related to the installation of software updates.
3) For scenarios where the installation of software updates is carried out by the manufacturer's representatives, the manufacturer shall provide evidence (e.g., SOPs, installation guides, instruction manuals, etc.) to demonstrate that standardised processes and procedures are available for the representatives to follow.

Assessment

- The assessor shall examine the evidence to verify that the manufacturer has procedures in place to notify device owners/operators on the availability of software updates.
- The assessor shall examine the software update guidance documents to determine that they are clear and easily understandable to facilitate 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 provides a standardised process and procedure for their representatives to follow when they perform the installation of software updates.

CSUP.3

The device shall only allow the installation of approved software.

Status

The provision is **mandatory**.

Intent of the Provision

The intent of this provision is to ensure that the device has mechanisms implemented that prevents the installation of unapproved software.

Minimum Requirements

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

Possible examples of how the device can allow the installation of approved software and/or applications, but not limited to the following:

- The device allows only the installation of software that is approved and digitally signed by manufacturer.
- The device employs privilege controls to prevent the installation of unapproved software by users.
- To prevent the installation of any software completely.

Supporting Evidence

- The manufacturer shall provide an explanation of how the mechanism implemented on the device prevents the installation of unapproved software.
- The manufacturer shall provide evidence (e.g., screenshots, videos, device documentation, etc.) to demonstrate the mechanism preventing the installation of unapproved software.

Assessment

- The assessor shall examine the evidence to determine that the mechanism is adequate in preventing the installation of unapproved software.

CSUP.4

The manufacturer shall have an on-going plan to proactively monitor and identify newly discovered cybersecurity vulnerabilities, assess their threat, and respond.

Status

The provision is **mandatory**.

This provision is taken to be fulfilled if the 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 in place a plan to proactively monitor, identify, and assess the device vulnerabilities regularly.

Minimum Requirements

- The manufacturer shall have processes in place to monitor sources (e.g., CVE databases [CVE list, NVD, etc.] and ISACs/ISAOs) to proactively identify vulnerabilities that may be relevant to the device.
- There shall be a process to verify if the device is susceptible to the identified potential vulnerability.
- For all vulnerabilities that are verified, the manufacturer shall perform threat and risk assessment (TRA) to ascertain the impact it can have on the device and to assign a severity rating to each of them (e.g., critical, high, medium, low, etc.).

Supporting Evidence

1) The manufacturer shall provide the sources that are actively monitored to identify vulnerabilities that may be relevant to the device.
2) The manufacturer shall provide supporting evidence (e.g., internal process documents, etc.) demonstrating the presence of a process to verify if the device is susceptible to any identified potential vulnerabilities.
3) The manufacturer shall provide supporting evidence (e.g., internal process documents, etc.) demonstrating the presence of a process to perform TRA on verified vulnerabilities in (2).
4) The manufacturer shall provide the severity rating(s) (e.g., critical, high, medium, low, etc.) used for the categorisation of vulnerabilities.

Assessment

- The assessor shall check that the manufacturer has processes in place to monitor sources and proactively identify vulnerabilities that may be relevant to the device.
- The assessor shall check that the manufacturer has processes in place to verify if the device is susceptible to any identified potential 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 handles data needed for further processing/storing, the device shall provide the capability for the data to be backed up to remote storage or removable media.

Status

The provision is **mandatory for devices that handles data needed for further processing/storing.**

Intent of the Provision

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

Minimum Requirements

- The device shall have the capability for data needed for further processing/storing to be backed up to remote storage or removable media.

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., product documentation, videos, etc.) demonstrating the device's capability to back up data that is needed for further processing/storing to remote storage or removable storage.

Assessment

- The assessor shall check that the 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.

Status

The provision is **mandatory for unconstrained devices.**

Intent of the Provision

The intent of this security provision is to ensure that the device supports the backing up of system configuration information as well as perform patch and software restoration.

Minimum Requirements

- The 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 device's capability to back up system configuration information.

2) The manufacturer shall provide evidence (e.g., product documentation, screenshots, etc.) demonstrating the device's capability 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 device shall have at least one malware protection measure/mechanism.

Status

The provision is **mandatory for unconstrained devices and for devices that makes use of operating systems.**

Intent of the Provision

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

Minimum Requirements

- The device shall have at least one malware protection measure/mechanism.

Possible examples of malware protection measures/mechanisms are, but not limited to the following:

- 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 device's malware protection measure/mechanism implementation.

    a. If the device utilises an anti-malware software, its name and version number shall be provided.

2) The manufacturer shall provide an explanation of how the malware protection measure/mechanism is adequate in protecting the device from malware.

Assessment

- The assessor shall examine the supporting evidence to determine that the manufacturer has implemented a malware protection measure/mechanism on the device.

- The assessor shall check that a reasonable explanation is given to justify that the malware protection measure/mechanism is adequate in protecting the device against malware.

NODE AUTHENTICATION (NAUT)

NAUT.1

The device shall have network access control measure/mechanism.

Status

The provision is **mandatory for devices that communicate with other devices.**

Intent of the Provision

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

Minimum Requirements

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

Possible examples of such capabilities are, but not limited to the following:

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

Supporting Evidence

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

2) The manufacturer shall provide an explanation of how the network access control measure/mechanism is adequate in only allowing access to permitted entities.

Assessment

- The assessor shall examine the evidence to determine that the manufacturer has implemented a network control measure/mechanism on the device.

- The assessor shall check that a reasonable explanation is given to justify that the network access control measure/mechanism is adequate in only providing network access to permitted entities.

CONNECTIVITY CAPABILITIES (CONN)

CONN.1

All communication channels supported by the device shall be declared.

Status

The provision is **mandatory for devices that communicate with other devices.**

Intent of the Provision

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

Minimum Requirements

- All the device's supported communication channels shall be accounted for. This includes communication channels that are not intended for the user's interactions (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 device are, but not limited to the following:

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

Supporting Evidence

1) The manufacturer shall provide a complete list of all communication channels supported by the device, clearly indicating its default status (enabled or disabled).

Assessment

- The assessor shall examine the list to determine that it is complete. The assessor may enhance the assessment by leveraging insights gained from the assessment of other security provisions and supporting evidence outlined in this document.

PERSON AUTHENTICATION (PAUT)

PAUT.1

The device shall support and enforce authentications for all users and roles.

Status

The provision is **mandatory.**

Intent of the Provision

The intent of this provision is to ensure that the device enforces authentications for all users and roles.

Minimum Requirements

- The manufacturer shall state the functionalities that are available on the device without authentication.
    - Note: Where applicable, the device may support medical functionalities (e.g., monitoring of patient statistics, medical emergencies, etc.) necessary for its intended use without authentication.

Supporting Evidence

1) The manufacturer shall provide a list of device functionalities that are available on the device without authentication, along with a corresponding rationale for why authentication is not required for these functionalities.

Assessment

- The assessor shall examine the list of device functionalities that do not require authentication and the corresponding rationale to determine that the functionalities do not necessitate authentication.

PAUT.2

The device shall support the changing of authentication values (e.g., passwords, PINs, biometrics, etc.) for all users and roles.

Status

The provision is **mandatory for devices that support authentication.**

Intent of the Provision

The intent of this provision is to ensure that the device provides the capability for device owners/operators to change the 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.), there shall be comprehensive guidance provided to the device owner/operator to assist them.

Supporting Evidence

1) For each of the device's authentication interface as indicated in PAUT.1, the manufacturer shall provide evidence (e.g., screenshots, videos, user guidance documents, device documentations, etc.) to show how 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 given to device owners/operators to change authentication values for all users and roles.

Assessment

- The assessor shall examine the evidence to determine that the device supports the changing authentication values for all users and roles.
- For cases where the process of changing authentication values is not easily understandable or straightforward, the assessor shall check that comprehensive guidance is given to device owners/operators to change authentication values for all users and roles.

PAUT.3

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

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

Status

The provision is **mandatory** for devices that supports password or PIN-based authentication.

Intent of the Provision

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

Minimum Requirements

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.

These requirements encompass passwords used by the underlying operating system, meaning that these requirements also extend to the operating system credentials for medical software running of the platform.

Other requirements:

- For all authentication where credentials are required to be transmitted shall be performed over a secure communication channel. Acceptable examples

include, but not limited to:

- TLS 1.2 or higher, with acceptable cipher suites (refer to NIST SP 800-52).
- 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 list all the device's authentication interface(s) that are enabled by default (e.g., device administrator portal, companion mobile application, telnet, FTP, SSH, etc.) and state which category (below) their corresponding passwords/PINs fall within:
    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 passwords examples that were generated using the password generation method stated above.
3) For pre-installed passwords/PINs that are not unique:
    a. The manufacturer shall provide supporting evidence (e.g., user manuals, screenshots, videos, etc.) that shows or describes the device's setup process explicitly showing/stating that the device will not enter an operationalised state before the user defines a new password/PIN.
4) No pre-installed passwords/PINs:
    a. The manufacturer shall provide supporting evidence (e.g., user manuals, screenshots, videos, etc.) that shows or describes the device's setup process explicitly showing/stating that the device will not enter an operationalised state before the user defines a new password/PIN.
5) The manufacturer shall provide evidence to demonstrate the secure transmission of credentials between entities using best practice cryptography.
    a. For TLS Implementations, refer to **Annex A** for more information.

Assessment

- The assessor shall check that the list of authentication interfaces which are enabled by default is complete and if all the corresponding 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 determine that the device will not enter an operationalised state until a new password/PIN is defined.
- The assessor shall examine the evidence to ensure that credentials are transmitted securely using best practice cryptography.

PAUT.4

The device shall have a mechanism available which makes brute-force attacks on authentication interfaces via logical interfaces impractical.

Status

The provision is **mandatory** for devices which support authentication.

Intent of the Provision

The intent of the provision is to ensure that the device's authentication interfaces are not susceptible to brute-force attacks.

Minimum Requirements

- All the device's authentication interfaces (e.g., device administrator portal, companion mobile application, FTP, SSH, etc) shall employ a brute-force attack prevention measure. Examples of typical brute-force prevention measures are, but not limited to the following:
    - Rate limiting policies that limit the number of authentications within an interval (e.g., locks/delays enforced after a threshold is met, etc.).
    - Using multi-factor authentication (MFA) after initial setup.
    - Requiring One-Time-Passwords/PINs (OTPs).
    - Account lockout until hardware reset.
    - Account lockout until enabled in webGUI admin portal.
- For instances where a rate limiting policy is employed as a brute-force attack prevention measure, it shall meet the following requirements:
    - If a delay is enforced after a threshold is met, it shall require **at least 100 days** to compromise via a brute-force attack.
    - If IP blocking is enforced, the chance of a brute-force attack being successful shall be **lower than 1%.**

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.) and its corresponding authentication mechanism (e.g., passwords, tokens, digital signatures, biometrics, etc.) on the device.
2) The manufacturer shall describe the brute-force prevention measure implemented on each of the device's authentication interfaces mentioned in 1).
3) For brute-force prevention measures that are not rate limiting policies, the manufacturer shall provide supporting evidence (e.g., screenshots of OTPs process, documentation, login validity period after OTP requested, etc.) showing how it works.
4) For rate limiting policies, the manufacturer shall provide the following:
    a. State the maximum number of attempts (the threshold) within a given period (or attempts per IP address) and the result of reaching it (e.g., explain what happens after hitting the threshold – IP blocked, delay enforced, etc.).

b. Provide 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. The manufacturer shall perform the calculation using the formula indicated below to show that the rate limiting policy employed meets the requirements stated above.

Number of Days required	$\frac{Password\ Character\ Pool^{(Password\ Length)}}{Number\ of\ tries\ in\ 24hrs\ \times\ 2}$
% chance of brute-force attack succeeding	$\frac{Number\ of\ IP\ addresses\ \times Tries\ per\ IP\ address}{Password\ Character\ Pool^{(Password\ Length)}} \times 100\%$

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 that are not 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 check/examine the following:

  - If the manufacturer stated a threshold and a result of reaching that threshold (e.g., enforcing a delay on the authentication interface, IP blocked, etc.).

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

  - If the calculation provided by the manufacturer shows that the rate limiting policy employed on the authentication interface meets the requirements stated above.

ROADMAP FOR MEDICAL DEVICE LIFE CYCLE (RDMP)

RDMP.1

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

Status

The provision is **mandatory**.

This provision is taken to be fulfilled if the 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 adopts a risk management process to address cybersecurity risks and to verify the security of the device and the effectiveness of its security controls.

Minimum Requirements

- Manufacturers shall have a risk management plan that identifies, assesses, and implements mitigations for the relevant cybersecurity risks or vulnerabilities. It shall also specify how the mitigation measures are monitored for their effectiveness.
- Testing shall be performed on the 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
- AAMI TIR57:2016/(R) 2019 — Principles for medical device security-Risk management

Supporting Evidence

1) The manufacturer shall provide their risk management plan.
2) The manufacturer shall provide evidence to show that the security controls have been verified. Possible examples are, but not limited to the following:
    a. Description of test methodology, test results and conclusions.
    b. A traceability matrix between security risks, security controls, and testing to verify those controls.
    c. References to any standards and internal SOPs/documentation used.

Assessment

- The assessor shall examine the evidence to determine that the risk management plan adopted by the manufacturer has information on the following:
  - Identification, assessment, and implementation of mitigation for the relevant cybersecurity risks or vulnerabilities.
  - Monitoring of the effectiveness of implemented mitigation measures.
- The assessor shall examine the test reports or test documentation to determine that the security of the device and effectiveness of its security controls are verified.

RDMP.2

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

Status

The provision is **mandatory.**

Intent of the Provision

The intent of this provision is to ensure that the manufacturer adopts secure software development lifecycle processes during product development and puts in place a process to evaluate third-party applications and software components before they are integrated into the device.

Minimum Requirements

- The manufacturer shall adopt secure software development lifecycle processes, implementing at least one activity from each of the following categories. The manufacturer may also propose alternative activities related to these categories.
  - 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.

More information on secure software development lifecycle processes is available in the following publications:

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

Supporting Evidence

1) The manufacturer shall state if any secure software development lifecycle 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 the secure software development lifecycle processes have been adopted in the development of the device.

Assessment

- The assessor shall examine the evidence to determine that the manufacturer has adopted secure software development lifecycle processes.

RDMP.3

The manufacturer shall maintain a web page (or through other avenues) to provide information on software support period and updates.

Status

The provision is **mandatory.**

Intent of the Provision

The intent of this provision is to ensure that the manufacturer provides an avenue for device owners/operators to obtain information on the device's software support period and updates.

Minimum Requirements

- The device manufacturer shall maintain an avenue for disseminating information regarding 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, specifying a specific date (incl. day, month, and year) until which the manufacturer guarantees support for the device.

Supporting Evidence

1) The manufacturer shall provide the avenues that information is disseminated and shall provide evidence (e.g., screenshots, webpage URL, etc.) to show how information is provided to device owners/operators.

Assessment

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

RDMP.4

The manufacturer shall have a plan for managing third-party component end-of-life and end-of-support.

Status

The provision is **mandatory.**

Intent of the Provision

The intent of this provision is to ensure that the manufacturer has a process to manage the end-of-life (EOL) or end-of-support (EOS) of third-party components. It ensures that third-party components are monitored, and actions/measures can be executed when they reach EOL or EOS.

Minimum Requirements

- There shall be processes in place to manage third-party component EOL or EOS, consisting of all 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 by communicating with vendors or through 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 verify that the manufacturer's processes include the steps specified in the minimum requirements.

SOFTWARE BILL OF MATERIALS (SBOM)

SBOM.1

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

Status

The provision is **mandatory.**

Intent of the Provision

The intent of this provision is to ensure that the manufacturer maintains an SBOM for the device to facilitate the monitoring of components and its associated vulnerabilities. It would also assist in deploying more targeted updates/remediation measures to maintain the device's safety and essential functionality.

Minimum Requirements

- The SBOM shall cover all software and firmware components utilised by the device. This includes 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.
- For each of the software and firmware components identified in the SBOM(s), the following details shall be present:
  - Author of the SBOM.
  - Timestamp (date and time when the SBOM was last updated).
  - Component Name.
  - Component Version.
  - License Information.

Supporting Evidence

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

Assessment

- The assessor shall examine 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 device in accordance with industry standards.

Status

The provision is **mandatory.**

Intent of the Provision

The intent of this provision is to ensure that the manufacturer hardens the device in accordance with industry standards and best practices.

Minimum Requirements

- The device shall be hardened in accordance with industry standards and best practices.

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

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

Supporting Evidence

1) The manufacturer shall state the industry standard(s) and best practice(s) that was referenced in the hardening of the device.

2) The manufacturer shall describe the measures taken to harden the device and provide evidence (e.g., screenshots, device whitepapers, device information documents, etc.) to show its implementation.

Assessment

- The assessor shall check that the manufacturer has performed device hardening in accordance with industry standards and best practices.

- The assessor shall examine the evidence provided by the manufacturer to verify if there are measures taken to harden the device.

SAHD.2

The device shall employ mechanism for software integrity checking.

Status

The provision is **mandatory.**

Intent of the Provision

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

Minimum Requirements

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

Supporting Evidence

1) The manufacturer shall specify the software integrity checking mechanism(s) utilised, including the cryptographic algorithms used.

2) The manufacturer shall provide evidence (e.g., device whitepapers, device information documents, etc.) to show that the software integrity checking mechanism(s) mentioned in (1) is implemented on the device.

Assessment

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

SAHD.3

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

Status

The provision is **mandatory.**

Intent of the Provision

The intent of this provision is to ensure that all unused/unnecessary resources and services of the device are disabled to reduce its overall attack surface.

Minimum Requirements

- The device shall only have required resources and services enabled.

Examples of resources and services that shall be disabled or removed are, but not limited to the following:

- 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 list all resources and services that are available or enabled by default on the device and provide a rationale for its necessity.

Assessment

- The assessor shall examine the list to determine that there is a reasonable rationale to justify each available or enabled by default resources and services.

SAHD.4

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

Status

The provision is **mandatory.**

Intent of the Provision

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

Minimum Requirements

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

For informative purposes, a non-exhaustive list of the common communication ports and protocols used by medical devices can be found in the below:

- 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 list all network communication ports and protocols that are enabled by default on the device and provide a rationale for its 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 examine the list to determine that there is a reasonable rationale to justify each available or enabled by default network communication port and protocols.

- The assessor shall examine the NMAP scan output to determine 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 owner/operator.

Status

The provision is **mandatory**.

Intent of the Provision

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

Examples of guidance that can be provided to device owners/operators are, but not limited to:

- How to set up multi-factor authentication (if the device supports it).
- Guidance to configure access control mechanisms.
- User account and roles.
- Network access control.

The security documentation could be part of the device's installation/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 device owners/operators.

2) For devices that would be setup by the manufacturer's personnel (e.g., field service engineer, etc.), the documentation utilised by the manufacturer's personnel to perform the setup/configuration process shall also be provided.

Assessment

- The assessor shall examine the security documentation to determine that it provides sufficient guidance to device owners/operators to configure and operate the device securely.

SGUD.2

The device shall have the capability for the permanent deletion of sensitive or PII data from the device or media. The manufacturers shall provide the necessary instructions for this feature.

Status

The provision is **mandatory**.

Intent of the Provision

The intent of this provision is to ensure that the device provides owners/operators with the capability to permanently delete sensitive or PII data from the device or media when it is being decommissioned or if it is to be re-deployed.

Minimum Requirements

- For all data listed in MSD.1, the 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 them.

- The existence of the feature(s) along with information on how to use it shall be provided to device owners/operators.

Supporting Evidence

1) The manufacturer shall list all features that permanently deletes sensitive or PII data stored on the device or media.

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

Assessment

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

- The assessor shall examine the evidence to determine that the existence of device feature(s) along with information on how to use it, is provided to device owners/operators.

SGUD.3

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

Status

The provision is **mandatory**.

Intent of the Provision

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

Minimum Requirements

- The manufacturer shall provide device owners/operators with information on all pre-installed user accounts (including technician/service/administrator accounts, etc.).

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.

Assessment

- The assessor shall examine the evidence and determine that information on pre-installed user accounts are made available to device owners/operators.

HEALTH DATA STORAGE CONFIDENTIALITY (STCF)

STCF.1

The device shall support encryption of sensitive data at rest.

Status

The provision is **mandatory for unconstrained devices.**

Intent of the Provision

The intent of this provision is to ensure that all sensitive data is encrypted at rest.

Minimum Requirements

- The device shall have the capability to encrypt sensitive data at rest.
- Best practice cryptography shall be employed (refer to NIST SP 800-52 or NIST SP 800-131A).

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

- 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 the following:
    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 key.

Assessment

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

TRANSMISSION CONFIDENTIALITY (TXCF)

TXCF.1

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

Status

The provision is **mandatory for devices that can communicate with other devices.**

Intent of the Provision

The intent of this provision is to ensure that all sensitive data is protected using the best practice cryptography prior to transmission via a network or removable media.

Minimum Requirements

- The device shall have the capability to encrypt sensitive data using best practice cryptography prior to transmission via at network or removable media.

Acceptable examples are, but not limited to the following:

- The 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).
- 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.
- 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.) that the sensitive data is transmitted between.

   Possible examples of such communication are, but not limited to the following:
   - 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 stated above, the manufacturer shall provide evidence demonstrating the encryption of sensitive data prior to transmission. It shall include the following:

    a. 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. Provide 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 ensure that all communicating entities (e.g., devices, services, networks, etc.) where sensitive or PII data may be transmitted between is accounted for.

- For each communication stated in (1) of the supporting evidence provided by the manufacturer, the assessor shall check that the device is able to encrypt sensitive or PII data 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 is adequate in protecting 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 device shall support mechanisms (i.e., digital signatures, hash-based message authentication code) to ensure data is not modified during transmission.

Status

The provision is **mandatory for devices that can communicate with other devices.**

Intent of the Provision

The intent of this provision is to ensure that data is not modified during transmission, by using best practice cryptography.

Minimum Requirements

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

Examples of how data integrity during transmission could be ensured, not limited to the following:

- Transport Layer Security (TLS) 1.2 or higher, with acceptable cipher suites (refer to NIST SP 800-52)
- 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.).

   Possible examples of such communication are, but not limited to the following:
   - 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 stated above, the manufacturer shall provide evidence to show data integrity is ensured. Evidence provided here shall include the following:

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

Assessment

- The assessor shall examine the list to determine that all communicating entities are accounted for, and that the data integrity between each of the communicating entities are ensured.

REMOTE SERVICE (RMOT)

RMOT.1

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

Status

The provision is **mandatory if the device supports remote sessions.**

Intent of the Provision

The intent of this provision is to ensure that the device has the capability to indicate (or alert) the owner/operator when there is an incoming request for remote session and if there is an ongoing remote session. This helps device owners/operators in identifying possible unauthorised or suspicious remote session activities.

Minimum Requirements

- The device shall have the capability to inform device owners/operators when there is an incoming request for remote session.

- The device shall have the capability to inform device owners/operators if there are any ongoing remote sessions.

Examples of how the device can indicate these are, but not limited to the following:

- Session tracking mechanism to monitor and keep track of local and remote active user sessions.
- Remote session identification.
- Real-time alerting mechanisms 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.) to show that the device is able to indicate if there is an incoming request for remote session as well as if there are any ongoing remote sessions.

2) The manufacturer shall provide evidence (e.g., device whitepapers, screenshots, or videos of alerts/indicators during an active remote session, etc.) to show that the device is able to indicate if there is any ongoing remote sessions.

Assessment

- The assessor shall examine the evidence to determine that the device is able to indicate if there is an incoming request for a remote session.

- The assessor shall examine the evidence to determine that the device is able to indicate if there is an ongoing remote session.

OTHER SECURITY CONSIDERATIONS (OTHR)

OTHR.1

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

Status

The provision is **mandatory if the device supports remote sessions.**

Intent of the Provision

The intent of this provision is to ensure that the remote user performing remote administration on the device is authenticated and legitimate.

Minimum Requirements

- The device shall require the use of technical means to perform authentication prior to the initiation of the remote administration session.

Possible examples of using technical means to perform authentication are, but not limited to the following:

- 2-Factor Authentication (2FA).
- Multi-Factor Authentication (MFA).
- Dual-login (i.e., four-eyes principal approach where the session can only be initiated after both the remote user and local user have approved a request).

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

Possible examples of using procedural means to verify the identity of the remote user are, but not limited to the following:

- Phone/Video call to verify that all participating parties (e.g., remote user, local user, support representative, etc.) are legitimate.

Supporting Evidence

1) The manufacturer shall provide evidence (e.g., screenshots, documentation, etc.) outlining usage instructions of the technical or procedural means employed to authenticate or verify the identity of the remote administration user.

Assessment

- The assessor shall examine the evidence to determine that the employed technical or procedural mean to perform authentication is adequate in ensuring the authenticity and legitimacy of the remote user performing remote administration on the device.

OTHR.2

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

Status

The provision is **mandatory if the device supports Wi-Fi communications.**

Intent of the Provision

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

Minimum Requirements

- The device shall utilise the 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.) to show the Wi-Fi security protocols supported by the device.

2) The manufacturer shall declare if the Wi-Fi security protocols supported by the device, mentioned in (1), are enabled by default.

Assessment

- The assessor shall check that the device utilises the appropriate and recommended Wi-Fi security protocols and ensure 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 device shall be logically and/or physically disabled (i.e., tamper evident stickers, lindy port blockers) by default.

Status

The provision is **mandatory**.

Intent of the Provision

The intent of this provision is to ensure that unused local interfaces shall be logically or physically disabled to reduce the attack surface.

Minimum Requirements

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

Supporting Evidence

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

Assessment

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

ANNEX A – SUPPORTING EVIDENCE FOR TLS IMPLEMENTATION

In implementations where TLS is utilised. For each of the communicating entities mentioned, the manufacturer shall firstly 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 information below:

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

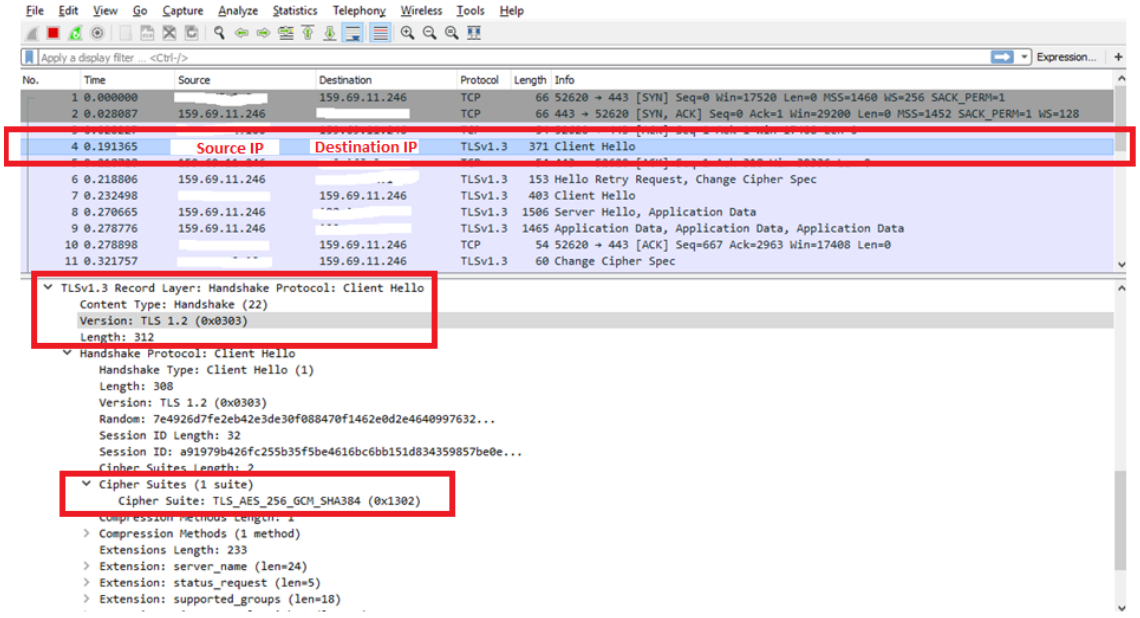

Image 2 – Highlighted information that should be included in the Wireshark screenshot

If the device plays the role of the server, the manufacturer shall provide a screenshot of the testssh.sh output showing all cipher suites that are supported by the device.

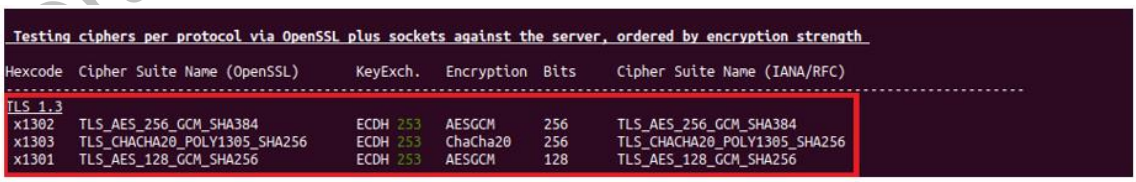

Image 2 – Highlighted information that should be included in the testssl.sh screenshot