

# Guidance for Medical Device Cybersecurity (GMDC)

---

GDHP Cyber Security Workstream



# CONTENTS

<b>GLOBAL DIGITAL HEALTH PARTNERSHIP GUIDANCE FOR MEDICAL DEVICE CYBERSECURITY (GMDC)</b> .....	<b>2</b>
1 INTRODUCTION.....	5
2 TARGET AUDIENCE.....	6
3 SCOPE OF GMDC.....	7
4 OVERVIEW OF GMDC.....	8
4.1. Provisions for each level.....	8
5 INSTRUCTIONS FOR USE.....	9
6 TERMS AND DEFINITION.....	10
7 ABBREVIATIONS.....	13
8 LEVEL 1 – BASELINE PROVISIONS.....	14
8.1. Overview.....	14
8.2. Declaration of Conformity to Baseline Provisions.....	14
8.3. Requirements.....	14
8.3.1. VULNERABILITY DISCLOSURE POLICY – VDP.1.....	15
8.3.2. CYBER SECURITY PRODUCT UPGRADES – CSUP.1.....	17
8.3.3. CYBER SECURITY PRODUCT UPGRADES – CSUP.4.....	19
8.3.4. PERSON AUTHENTICATION – PAUT.3.....	21
8.3.5. PERSON AUTHENTICATION – PAUT.4.....	24
8.3.6. ROADMAP FOR MEDICAL DEVICE LIFE CYCLE – RDMP.1.....	26
9 LEVEL 2 – Enhanced provisions.....	28
9.1. Overview.....	28
9.2. Declaration of Conformity to Enhanced Provisions.....	28
9.3. Requirements.....	29
9.3.1. MANAGEMENT OF SENSITIVE DATA – MSD.1.....	29
9.3.2. AUDIT CONTROLS – AUDT.1.....	31
9.3.3. AUDIT CONTROLS – AUDT.2.....	33
9.3.4. AUTHORIZATION – AUTH.1.....	35
9.3.5. AUTHORIZATION – AUTH.2.....	37
9.3.6. CYBER SECURITY PRODUCT UPGRADES – CSUP.2.....	39
9.3.7. CYBER SECURITY PRODUCT UPGRADES – CSUP.3.....	41
9.3.8. DATA BACKUP AND DISASTER RECOVERY – DTBK.1.....	43
9.3.9. DATA BACKUP AND DISASTER RECOVERY – DTBK.2.....	45
9.3.10. MALWARE DETECTION/PROTECTION – MLDP.1.....	47
9.3.11. NODE AUTHENTICATION – NAUT.1.....	49
9.3.12. CONNECTIVITY CAPABILITIES – CONN.1.....	51
9.3.13. PERSON AUTHENTICATION – PAUT.1.....	53
9.3.14. PERSON AUTHENTICATION – PAUT.2.....	55
9.3.15. ROADMAP FOR MEDICAL DEVICE LIFE CYCLE – RDMP.2.....	57
9.3.16. ROADMAP FOR MEDICAL DEVICE LIFE CYCLE – RDMP.3.....	60
9.3.17. ROADMAP FOR MEDICAL DEVICE LIFE CYCLE – RDMP.4.....	62
9.3.18. SOFTWARE BILL OF MATERIALS – SBOM.1.....	64
9.3.19. SYSTEM AND APPLICATION HARDENING – SAHD.1.....	66
9.3.20. SYSTEM AND APPLICATION HARDENING – SAHD.2.....	68
9.3.21. SYSTEM AND APPLICATION HARDENING – SAHD.3.....	70
9.3.22. SYSTEM AND APPLICATION HARDENING – SAHD.4.....	72
9.3.23. SECURITY GUIDANCE – SGUD.1.....	74
9.3.24. SECURITY GUIDANCE – SGUD.2.....	76
9.3.25. SECURITY GUIDANCE – SGUD.3.....	78
9.3.26. HEALTH DATA STORAGE CONFIDENTIALITY – STCF.1.....	80

9.3.27.	TRANSMISSION CONFIDENTIALITY– TXCF.1 .....	82
9.3.28.	TRANSMISSION INTEGRITY – TXIG.1 .....	84
9.3.29.	REMOTE SERVICE – RMOT.1 .....	86
9.3.30.	OTHER SECURITY CONSIDERATIONS – OTHR.1.....	88
9.3.31.	OTHER SECURITY CONSIDERATIONS – OTHR.2.....	90
9.3.32.	OTHER SECURITY CONSIDERATIONS – OTHR.3.....	92
<b>10</b>	<b><i>LEVEL 3 – Penetration testing</i></b> .....	<b>94</b>
10.1.	Overview .....	94
10.2.	Declaration of Conformity to Enhanced Provisions .....	94
10.3.	Software Binary Analysis and Penetration Testing .....	94
<b>11</b>	<b><i>LEVEL 4 – Advanced testing</i></b> .....	<b>95</b>
11.1.	Overview .....	95
11.2.	Declaration of Conformity to Enhanced Provisions .....	95
11.3.	Software Binary Analysis and Security Evaluation .....	95
<b>12</b>	<b><i>REFERENCES</i></b> .....	<b>96</b>



# 1 INTRODUCTION

The Global Health Digital Partnership (GDHP) is a collaboration of country governments and the World Health Organization (WHO) formed to support the executive implementation of worldwide digital health services. GDHP aims to facilitate international best practices in the use of data and technology to advance health and care, provides opportunities for policy co-production and knowledge transfer, and facilitates horizon scanning to forecast emerging trends more accurately.

In particular, the GDHP Cyber Security Workstream focuses on strategies that can strengthen the processes and practices designed to protect healthcare related devices, systems, and networks, as well as the data within them, from security risks and cyberattacks.

This Guidance for Medical Device Cybersecurity (GMDC) is an openly available, sound practice resource for medical device developers/manufacturers and healthcare purchasers to uplift cybersecurity posture through secure deployment and usage of medical devices.

## 2 TARGET AUDIENCE

Through recommending cybersecurity provisions for medical devices tiered into 4 levels, the GMDC serves to guide medical device manufacturers (MDMs) on developing secure-by-design products.

In addition, GMDC equips healthcare delivery organisations (HDOs) to identify the most pertinent cybersecurity features that they should consider and assess when deploying and using medical devices in the clinical setting.

HDO can also use it as a declaration of conformity by manufacturers to perform risk assessments as part of their procurement efforts.

### 3 SCOPE OF GMDC

The scope of the GMDC applies to medical devices and have any of the following characteristics:

- Handles personal identifiable information (PII) and clinical data and has the ability to collect, store, process, or transfer such data;
- Connects to other devices, systems, and services - Has the ability to communicate using wired and/or wireless communication protocols through a network of connections.

Medical devices referred in this document can be described as any instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article that is intended by its manufacturer to be used, whether alone or in combination, for humans for one or more of the specific purposes of —

(a)

- (i) diagnosis, prevention, monitoring, treatment or alleviation of disease;
- (ii) diagnosis, monitoring, treatment or alleviation of, or compensation for, an injury;
- (iii) investigation, replacement, modification or support of the anatomy or of a physiological process, mainly for medical purposes;
- (iv) supporting or sustaining life;
- (v) control of conception;
- (vi) disinfection of medical devices; or
- (vii) providing information by means of in vitro examination of specimens derived from the human body, for medical or diagnostic purposes,

and which does not achieve its primary intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its intended function by such means; and

(b) the following articles:

- (i) any implant for the modification or fixation of any body part;
- (ii) any injectable dermal filler or mucous membrane filler;
- (iii) any instrument, apparatus, implement, machine or appliance intended to be used for the removal or degradation of fat by invasive means.”.

## 4 OVERVIEW OF GMDC

The GMDC comprises four (4) medical device cybersecurity levels, with each higher level being more comprehensive in the assessment. These requirements are titrated from regulatory requirements from International Medical Device Regulatory Forum (IMDRF), NEMA Manufacturer Disclosure Statement for Medical Device Security (MDS2), NIST framework and ISO/IEC and TR67 standards. The 4 levels are adapted from Cybersecurity Labelling Scheme for Medical Device [CLS(MD)] framework that is progressively tiered from Level 1 to provide increasing security assurance as they attain compliance to higher levels.

### 4.1. PROVISIONS FOR EACH LEVEL

Table 1 details the recommended provisions per each medical device cybersecurity levels.

Level	Requirements	Recommended Provisions
1	Baseline Provisions	VDP.1, CSUP.1, CSUP.4, PAUT.3, PAUT.4, RDMP.1
2	Enhanced Provisions	6 baseline provisions and 32 enhanced provisions.
3	Penetration Testing	Enhanced provisions, software binary analysis and penetration testing
4	Advanced Testing	Enhanced provisions, software binary analysis and security evaluation

Table 1 - Provisions for each cybersecurity level



## 5 INSTRUCTIONS FOR USE

Manufacturers may also use this GMDC as a form to indicate conformity against each of the security provisions.

HDOs may use declaration of conformity by manufacturers to assess device conformity to requirements and perform risk assessments.

Alternatively, manufacturers can apply to [Cyber Security Labelling Scheme \[CLS\(MD\)\]](#) to be formally evaluated and labelled.

Manufacturer Contact Details	
Legal Entity Name	
Device Proprietary / Brand Name	
Medical Device Model and Version	
[Link (URL) to primary website]	
[Security Contact Name]	
[Security Contact Email Address]	
[Security Contact Phone Number]	
[Address; <i>minimum, Country</i> ]	

## 6 TERMS AND DEFINITION

Sensitive Security Parameters	<p>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.</p> <p>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.</p>
Critical Security Parameters	<p>Critical security parameters used for integrity and authenticity checks of software updates shall be unique per device.</p> <p>Example: secret keys, private components of certificates, etc.</p>
Sensitive Data	<p>“Sensitive personal data" is data whose disclosure has a high potential to cause harm to the individual. Sensitive data include the following:</p> <p>Personally Identifiable Information (e.g., Patient’s full name, home address, national identification numbers, phone numbers, email addresses, etc.).</p> <p>Clinical Data (e.g., Patient’s health and medical history, etc.)</p> <p>Sensitive or Critical Security Parameters (e.g., cryptographic keys, digital certificates, access control lists, authentication tokens, login credentials, etc.)</p>
Personally Identifiable Information	<p>This refers to any information that can be used to identify, contact, or locate an individual.</p> <p>Examples: Full Name, Address, Email Address, Phone Number, Passport Number, Biometric data, etc.</p>
Clinical Data	<p>This refers to sensitive and confidential information related to an individual’s medical history, treatment, and health records.</p> <p>Examples: Electronic Health Records (EHR), Laboratory test results, Physician Notes, Medical history, Prescription records, etc.</p>
Authentication Interface	<p>Interfaces on the device (or its companion application/services) that requires user interaction for authentication.</p> <p>Examples: WebGUI login portal, Mobile application login page, etc.</p>

Authentication Mechanisms	<p>Credential that is utilised by the user to authenticate themselves to the device using an authentication interface.</p> <p>Examples: passwords, tokens, smart cards, digital signatures, biometrics, etc.</p>
Update Mechanisms	<p>Ways that a medical device can receive and install firmware updates.</p> <p>Examples: Automatic update and manual update feature found on the device.</p>
LDAP	<p>An open standard protocol that is commonly used to communicate with directory servers.</p>
COTS	<p>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</p>
Operating System	<p>An operating system (OS) is system software that manages computer hardware and software resources and provides common services for computer programs.</p> <p>Examples of Operating Systems not limited to the following:</p> <ul style="list-style-type: none"> <li>- Microsoft Windows</li> <li>- Linux</li> <li>- Real-time operating systems (e.g., FreeRTOS, SafeRTOS, VxWorks, Nucleus, QNX, etc.).</li> </ul>
Access Control Mechanisms	<p>Security measures that regulate and manage access to resources, systems, or data within an organization's environment.</p> <p>Examples: Access control list (ACLs), role-based access control (RBAC) or multi-factor authentication (MFA).</p>
Anti-malware Software	<p>Software designed to detect, prevent, and remove malicious software, such as viruses, worms, and ransomware, from computer systems and networks, thereby enhancing cybersecurity protection.</p> <p>Examples: Antivirus software, anti-spyware software or endpoint detection and response (EDR) solutions.</p>

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

## 7 ABBREVIATIONS

CVE	Common Vulnerabilities and Exposures
DUT	Device Under Test
LDAP	Lightweight directory access protocol
MAC	Media Access Control Address
MFA	Multi-Factor Authentication
PII	Personal Identifiable Information
SOP	Standard Operating Procedure
VDP	Vulnerability Disclosure Process

## 8 LEVEL 1 – BASELINE PROVISIONS

### 8.1. OVERVIEW

The objective of Level 1 is to determine that the Device Under Test (DUT) conforms to a minimal set of baseline security requirements.

Level 1 is based solely on declaration of conformity by the Manufacturer.

Devices that have completed Level 1 would entail that the manufacturer has:

- i. considered cybersecurity risks and vulnerabilities as part of an overall risk management process throughout the lifecycle of the medical device.
- ii. has taken steps to avoid the use of universal default password.
- iii. has a vulnerability disclosure policy in place to manage vulnerability reporting.
- iv. has an on-going plan to proactively monitor and identify newly discovered vulnerabilities, and to remediate these vulnerabilities to ensure performance and safety of the device throughout the device's lifecycle.

### 8.2. DECLARATION OF CONFORMITY TO BASELINE PROVISIONS

Manufacturers may use the “Manufacturer’s declaration’ section within each provision to indicate conformity and provide the relevant support evidence.

### 8.3. REQUIREMENTS

This section provides clarification on the expectations for the 6 baseline provisions.

Each security provision is structured in the following manner:

- **Description of Security Provision** – Key components of security 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.
- **Reference** – Specify where security provision is adapted from.
- **Manufacturer’s declaration** – Manufacturers can use this section to indicate the supporting evidence for their device.

## VULNERABILITY DISCLOSURE POLICY – VDP.1

### Description of provision

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

### 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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) DOC-8
2. IMDRF (International Medical Device Regulators Forum) (2020). Principles and Practices for Medical Device Cybersecurity.

### Manufacturer's declaration

Yes

No

Not Applicable

**Supporting evidence:**



## CYBER SECURITY PRODUCT UPGRADES – CSUP.1

### Description of provision

*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.*

### 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

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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) CSUP-11
2. IMDRF (International Medical Device Regulators Forum) (2020). Principles and Practices for Medical Device Cybersecurity.

### Manufacturer's declaration

- Yes
- No
- Not Applicable

Supporting evidence:

## CYBER SECURITY PRODUCT UPGRADES – CSUP.4

### Description of provision

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

### 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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) CSUP-11
2. IMDRF (International Medical Device Regulators Forum) (2020). Principles and Practices for Medical Device Cybersecurity.

### Manufacturer's declaration

Yes

No

Not Applicable

**Supporting evidence:**

## PERSON AUTHENTICATION – PAUT.3

### Description of provision

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.

### 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:

<p>Pre-Installed Passwords/PINs that are <u>unique per device</u></p>	<ul style="list-style-type: none"> <li>• Pre-installed passwords/PINs shall be different across different units of the same device model.</li> <li>• Pre-installed passwords/PINs shall be randomised using a random function.</li> <li>• 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.).</li> <li>• Pre-installed passwords/PINs shall not have incremental counters (e.g., “password1”, “password2”, “password3”, etc.).</li> <li>• Pre-installed passwords/PINs shall not have common strings or patterns (e.g., “Password123”, “QWERTY”, etc.).</li> </ul>
<p>Pre-installed passwords/PINs that are not unique</p>	<ul style="list-style-type: none"> <li>• 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.</li> </ul>
<p>No pre-installed passwords/PINs</p>	<ul style="list-style-type: none"> <li>• 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.</li> </ul>

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.

**Reference**

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) PAUT-1
2. IMDRF (International Medical Device Regulators Forum) (2020). Principles and Practices for Medical Device Cybersecurity.

3. NIST SP 800-53 Rev. 4 IA-2

**Manufacturer's declaration**

Yes

No

Not Applicable

**Supporting evidence:**

## PERSON AUTHENTICATION – PAUT.4

### Description of provision

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

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

**Reference**

Adapted from

1. IEC 62443-4-2:2018, Section 5.13 - CR 1.11 – Unsuccessful login attempts

**Manufacturer’s declaration**

Yes  
 No  
 Not Applicable

**Supporting evidence:**

## ROADMAP FOR MEDICAL DEVICE LIFE CYCLE – RDMP.1

### Description of provision

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

### 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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) RDMP-1

2. IMDRF (International Medical Device Regulators Forum) (2020). Principles and Practices for Medical Device Cybersecurity.
3. NIST SP 800-53 Rev. 4 CM-2

**Manufacturer's declaration**

- Yes
- No
- Not Applicable

**Supporting evidence:**

## 9 LEVEL 2 – ENHANCED PROVISIONS

### 9.1. OVERVIEW

The objective of this activity is to determine that the Device Under Test (DUT) conforms to a set of enhanced security requirements.

Level 2 is based solely on declaration of conformity by the Manufacturer.

Devices that have completed Level 2 would entail that the manufacturer has conform to a set of 38 security requirements. The enhanced security requirements consist of the following:

- Level 1 baseline provisions
- Cybersecurity requirements covering areas such as:
  - Vulnerability Disclosure Policy
  - Management of Sensitive Data
  - Audit Controls
  - Authorisation
  - Cyber Security Product Upgrades
  - Data Backup and Disaster Recovery
  - Malware Detection/Protection
  - Node Authentication
  - Connectivity Capabilities
  - Person Authentication
  - Roadmap for Medical Device Life Cycle
  - Software Bill of Materials
  - System and Application Hardening
  - Security Guidance
  - Health Data Storage Confidentiality
  - Transmission Confidentiality
  - Transmission Integrity
  - Remote Service
  - Other security considerations.

### 9.2. DECLARATION OF CONFORMITY TO ENHANCED PROVISIONS

Manufacturers may use the “Manufacturer’s declaration’ section within each provision to indicate conformity and provide the relevant support evidence.

### 9.3. REQUIREMENTS

For requirements within the Level 1 baseline provisions, please refer to section 8.3. This section covers the rest of the 32 enhanced provisions.

<b>MANAGEMENT OF SENSITIVE DATA – MSD.1</b>
<b>Description of provision</b>
<i>The manufacturer shall maintain a list of sensitive data (such as personal identifiable information) that is collected and transmitted/transferred by the device.</i>
<b>Intent of the Provision</b>
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.
<b>Minimum Requirement</b>
<ul style="list-style-type: none"><li>• There shall be a maintained list of all sensitive data that is either collect by the device or transmitted/transferred by the device.</li><li>• The device shall only collect or transmit/transfer sensitive data when necessary.</li></ul> <p>Sensitive data is defined as the following:</p> <ul style="list-style-type: none"><li>• Personally Identifiable Information (e.g., Patient’s full name, home address, national identification numbers, phone numbers, email addresses, etc.).</li><li>• Clinical Data (e.g., Patient’s health and medical history, etc.)</li><li>• Sensitive or Critical Security Parameters (e.g., cryptographic keys, digital certificates, access control lists, authentication tokens, login credentials, etc.)</li></ul>
<b>Supporting Evidence</b>
<ol style="list-style-type: none"><li>1. The manufacturer shall provide a list of all sensitive data collected by the device.<ol style="list-style-type: none"><li>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.).</li></ol></li><li>2. For each sensitive data listed in (1), the manufacturer shall provide the rationale for the necessity on its the collection and transmission.</li><li>3. If the device does not collect or transmit/transfer sensitive data, the manufacturer shall provide a statement confirming this.</li></ol>
<b>Reference</b>
Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) MPII 2. NIST SP 800-53 Rev. 4 AR-2
<b>Manufacturer's declaration</b>
<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not Applicable  <b>Supporting evidence:</b>

## AUDIT CONTROLS – AUDT.1

### Description of provision

*The 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 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 Requirement

- 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.

### Reference

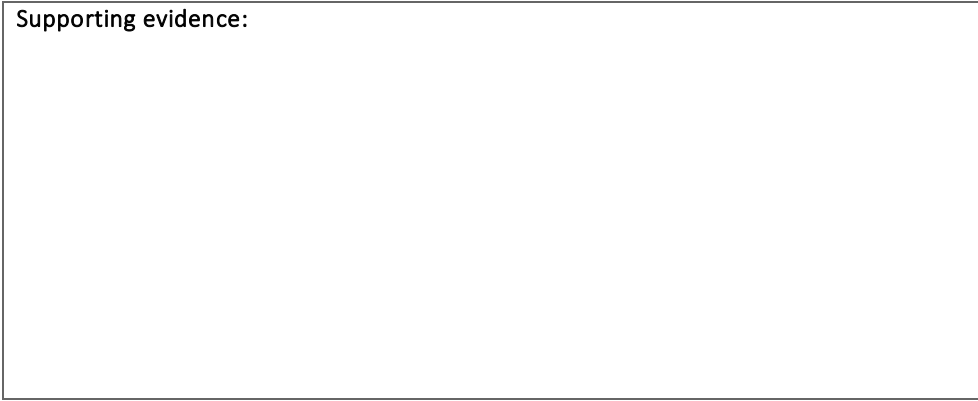
Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) AUDT-1
2. IEC TR 80001-2-2:2012 Section 5.2
3. NIST SP 800-53 Rev. 4 AU-1

### Manufacturer's declaration

- Yes
- No
- Not Applicable

Supporting evidence:





## AUDIT CONTROLS – AUDT.2

### Description of provision

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

### 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 Requirement

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

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

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) AUDT-2
2. IEC TR 80001-2-2:2012 Section 5.2
3. NIST SP 800-53 Rev. 4 AU-2

### Manufacturer's declaration

Yes

No

Not Applicable

**Supporting evidence:**

## AUTHORIZATION – AUTH.1

### Description of provision

*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.*

### 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.

### Reference

Adapted from

Manufacturer Disclosure Statement for Medical Device Security (MDS2) AUTH-1

IEC TR 80001-2-2:2012 Section 5.3

NIST SP 800-53 Rev. 4 IA-2

### Manufacturer’s declaration

Yes

No

Not Applicable

**Supporting evidence:**

## AUTHORIZATION – AUTH.2

### Description of provision

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

### 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.

### Reference

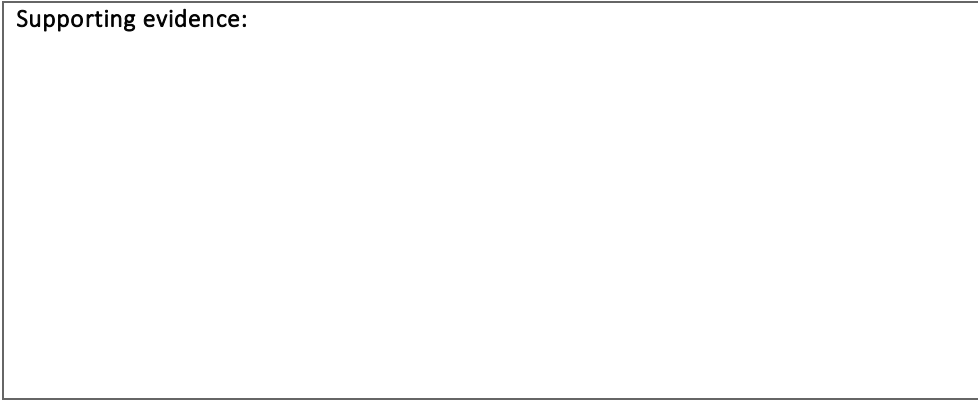
Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) AUTH-2
2. IEC TR 80001-2-2:2012 Section 5.3
3. NIST SP 800-53 Rev. 4 IA-2

### Manufacturer's declaration

- Yes
- No
- Not Applicable

Supporting evidence:



## CYBER SECURITY PRODUCT UPGRADES – CSUP.2

### Description of provision

*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.*

### 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.

**Reference**

Adapted from

Manufacturer Disclosure Statement for Medical Device Security (MDS2) CSUP-2 to CSUP-7

**Manufacturer's declaration**

Yes

No

Not Applicable

**Supporting evidence:**



## CYBER SECURITY PRODUCT UPGRADES – CSUP.3

### Description of provision

*The device shall only allow installation of approved software.*

### 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

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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) CSUP-10.1

**Manufacturer's declaration**

Yes

No

Not Applicable

**Supporting evidence:**

## DATA BACKUP AND DISASTER RECOVERY – DTBK.1

### Description of provision

*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.*

### 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

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.

### Reference

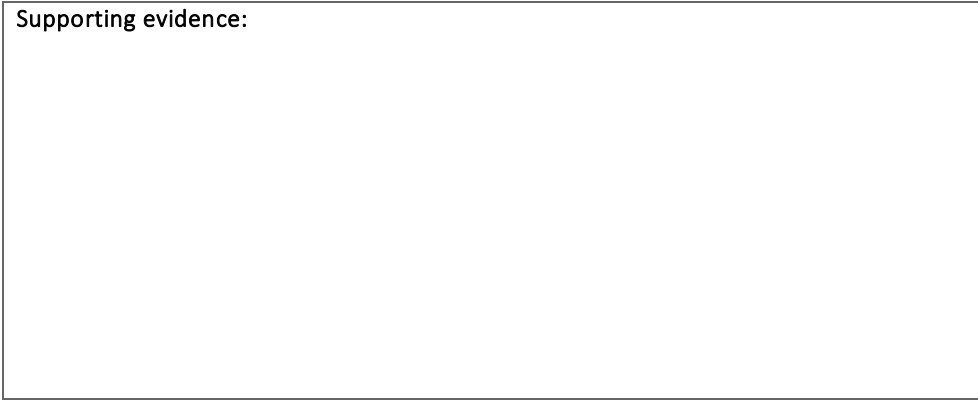
Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) DTBK-3, DTBK-4
2. IEC TR 80001-2-2:2012 Section 5.7
3. NIST SP 800-53 Rev. 4 CP-9

### Manufacturer's declaration

- Yes
- No
- Not Applicable

Supporting evidence:



## DATA BACKUP AND DISASTER RECOVERY – DTBK.2

### Description of provision

*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 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

- The manufacturer shall provide evidence (e.g., product documentation, screenshots, etc.) demonstrating the device's capability to back up system configuration information.
- The manufacturer shall provide evidence (e.g., product documentation, screenshots, etc.) demonstrating the device's capability to perform patch and software restoration.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) DTBK-5

### Manufacturer's declaration

- Yes
- No
- Not Applicable

**Supporting evidence:**



## MALWARE DETECTION/PROTECTION – MLDP.1

### Description of provision

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

### 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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) MLDP-2
2. IEC TR 80001-2-2:2012 Section 5.10
3. NIST SP 800-53 Rev. 4 SI-3

**Manufacturer's declaration**

Yes

No

Not Applicable

**Supporting evidence:**



## NODE AUTHENTICATION – NAUT.1

### Description of provision

*The device shall have network access control measure/mechanism.*

### 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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) NAUT-2
2. IEC TR 80001-2-2:2012 Section 5.11
3. NIST SP 800-53 Rev. 4 SC-7

### Manufacturer's declaration

Yes

No

Not Applicable

**Supporting evidence:**

## CONNECTIVITY CAPABILITIES – CONN.1

### Description of provision

*All communication channels supported by the device shall be declared.*

### 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

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

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) CONN-1 to CONN-7

**Manufacturer's declaration**

Yes

No

Not Applicable

**Supporting evidence:**

## PERSON AUTHENTICATION – PAUT.1

### Description of provision

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

### 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

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.

### Reference

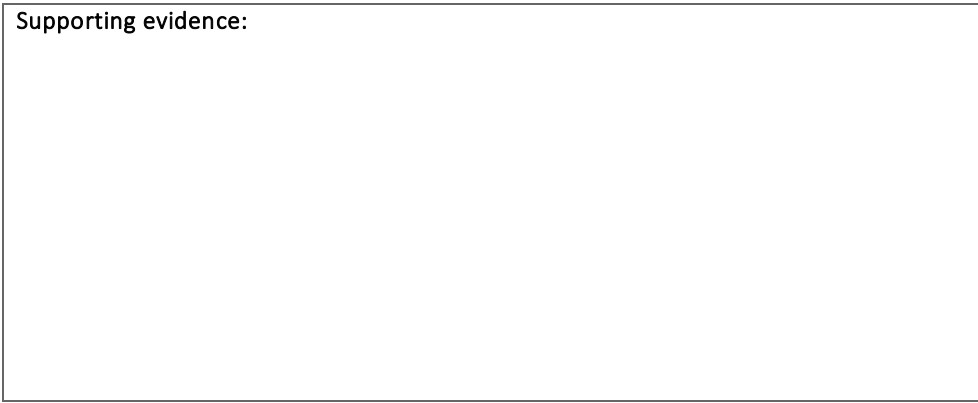
Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) PAUT-1
2. IEC TR 80001-2-2:2012 Section 5.12
3. NIST SP 800-53 Rev. 4 IA-2

### Manufacturer's declaration

- Yes
- No
- Not Applicable

Supporting evidence:

A large, empty rectangular box with a thin black border, intended for providing supporting evidence. The box is positioned in the upper left quadrant of the page.

## PERSON AUTHENTICATION – PAUT.2

### Description of provision

*The device shall support the changing of 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 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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) PAUT-5
2. IEC TR 80001-2-2:2012 Section 5.12

### Manufacturer's declaration

Yes

No

Not Applicable

**Supporting evidence:**



## ROADMAP FOR MEDICAL DEVICE LIFE CYCLE – RDMP.2

### Description of provision

*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.*

### 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

<ul style="list-style-type: none"> <li>○ Implementing an evaluation process to assess third-party applications and software components for its security. <ul style="list-style-type: none"> <li>- Assessing track record of third-party applications and software components, including known vulnerabilities and security incidents</li> <li>- Ensuring that security controls implemented by third-party vendors for these components are adequate for the device.</li> </ul> </li> <li>○ Conducting software composition analysis.</li> <li>● <u>Functional Testing</u> <ul style="list-style-type: none"> <li>○ Conducting unit and integration tests.</li> </ul> </li> <li>● <u>Security Testing</u> <ul style="list-style-type: none"> <li>○ Performing threat mitigative testing.</li> <li>○ Performing vulnerability testing, including malformed or unexpected input testing, and the use of vulnerability scanning tools.</li> <li>○ Conducting penetration tests.</li> </ul> </li> </ul> <p>More information on secure software development lifecycle processes is available in the following publications:</p> <ul style="list-style-type: none"> <li>● ISO/IEC 81001-5-1 “Health informatics – Management and governance of health software systems – Part 5-1: Health software system safety, security and performance”</li> <li>● U.S. Food and Drug Administration – FDA-2021-D-1158 - “Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions”</li> <li>● EU MDCG 2019-16 Rev.1 “Guidance on Cybersecurity for medical devices”</li> <li>● ISO 27034-1:2011 “Information Security – Security Techniques – Application security Part 1: Overview and concepts”</li> <li>● IEC 62304:2006 “Medical device software – Software life cycle processes”</li> <li>● ISO 13485:2016 “Medical devices – Quality management systems – Requirements for regulatory purposes”</li> </ul>
<b>Supporting Evidence</b>
<ol style="list-style-type: none"> <li>1. The manufacturer shall state if any secure software development lifecycle publications have been referenced or adopted.</li> <li>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.</li> </ol>
<b>Reference</b>
<p>Adapted from</p> <ol style="list-style-type: none"> <li>1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) RDMP-2</li> <li>2. IEC TR 80001-2-2:2012 Section 5.14</li> <li>3. NIST SP 800-53 Rev. 4 CM-2, CM-8</li> </ol>

**Manufacturer's declaration**

Yes

No

Not Applicable

**Supporting evidence:**

## ROADMAP FOR MEDICAL DEVICE LIFE CYCLE – RDMP.3

### Description of provision

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

### 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

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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) RDMP-3
2. IEC TR 80001-2-2:2012 Section 5.14
3. NIST SP 800-53 Rev. 4 CM-8

### Manufacturer's declaration

Yes

No

Not Applicable

**Supporting evidence:**

## ROADMAP FOR MEDICAL DEVICE LIFE CYCLE – RDMP.4

### Description of provision

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

### 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

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.

## Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) RDMP-4
2. IEC TR 80001-2-2:2012 Section 5.14
3. NIST SP 800-53 Rev. 4 CM-8

## Manufacturer's declaration

Yes

No

Not Applicable

**Supporting evidence:**

## SOFTWARE BILL OF MATERIALS – SBOM.1

### Description of provision

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

### 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

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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) SBOM-1



2. IMDRF (International Medical Device Regulators Forum) (2020). Principles and Practices for Medical Device Cybersecurity.

**Manufacturer's declaration**

Yes

No

Not Applicable

**Supporting evidence:**

## SYSTEM AND APPLICATION HARDENING – SAHD.1

### Description of provision

*The manufacturer shall harden the device in accordance to industry standards.*

### 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

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

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) SAHD-1
2. IEC TR 80001-2-2:2012 Section 5.15

**Manufacturer's declaration**

Yes

No

Not Applicable

**Supporting evidence:**

## SYSTEM AND APPLICATION HARDENING – SAHD.2

### Description of provision

*The device shall employ mechanism for software integrity checking.*

### 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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) SAHD-3

### Manufacturer's declaration

- Yes
- No
- Not Applicable

Supporting evidence:

A large, empty rectangular box with a thin black border, occupying the upper half of the page. It is positioned to the right of the text 'Supporting evidence:'. This box is intended for the user to provide supporting evidence for their response.

## SYSTEM AND APPLICATION HARDENING – SAHD.3

### Description of provision

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

### 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

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.

### Reference

- Adapted from
1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) SAHD-7
  2. IEC TR 80001-2-2:2012 Section 5.15
  3. NIST SP 800-53 Rev. 4 CM-7

### Manufacturer's declaration

Yes

No

Not Applicable

**Supporting evidence:**

**Description of provision**

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

**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>`

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) SAHD-8, SAHD-9
2. IEC TR 80001-2-2:2012 Section 5.15
3. NIST SP 800-53 Rev. 4 CM-7

### Manufacturer's declaration

- Yes
- No
- Not Applicable

**Supporting evidence:**

## SECURITY GUIDANCE – SGUD.1

### Description of provision

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

### 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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) SGUD-1
2. IEC TR 80001-2-2:2012 Section 5.16
3. NIST SP 800-53 Rev. 4 SA-5

**Manufacturer's declaration**

Yes

No

Not Applicable

**Supporting evidence:**

## SECURITY GUIDANCE – SGUD.2

### Description of provision

*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.*

### 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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) SGUD-2
2. IEC TR 80001-2-2:2012 Section 5.16
3. NIST SP 800-53 Rev. 4 MP-6

### Manufacturer's declaration

Yes

No

Not Applicable

**Supporting evidence:**

## SECURITY GUIDANCE – SGUD.3

### Description of provision

*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.*

### 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

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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) SGUD-3
2. IEC TR 80001-2-2:2012 Section 5.16
3. NIST SP 800-53 Rev. 4 AC-6, IA-2

### Manufacturer's declaration

- Yes
- No
- Not Applicable

Supporting evidence:

## HEALTH DATA STORAGE CONFIDENTIALITY – STCF.1

### Description of provision

*The 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 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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) STCF-1
2. IEC TR 80001-2-2:2012 Section 5.17
3. NIST SP 800-53 Rev. 4 SC-28



**Manufacturer's declaration**

Yes

No

Not Applicable

**Supporting evidence:**

## TRANSMISSION CONFIDENTIALITY– TXCF.1

### Description of provision

*The 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 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.

**Reference**

- Adapted from
1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) TXCF-2
  2. IEC TR 80001-2-2:2012 Section 5.18
  3. NIST SP 800-53 Rev. 4 SC-8

**Manufacturer’s declaration**

- Yes
- No
- Not Applicable

**Supporting evidence:**

## TRANSMISSION INTEGRITY – TXIG.1

### Description of provision

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

### 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.

**Reference**

Adapted from

Manufacturer Disclosure Statement for Medical Device Security (MDS2) TXIG-1

IEC TR 80001-2-2:2012 Section 5.19

NIST SP 800-53 Rev. 4 SC-8

**Manufacturer's declaration**

Yes

No

Not Applicable

**Supporting evidence:**

## REMOTE SERVICE – RMOT.1

### Description of provision

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

### 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 session(s).

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) RMOT-1.2

### Manufacturer's declaration

Yes

No

Not Applicable

**Supporting evidence:**

## OTHER SECURITY CONSIDERATIONS – OTHR.1

### Description of provision

*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.*

### 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.

- 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

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.

### Reference

Adapted from



1. IEC 62443-4-2:2018, Section 5.3, 5.4

**Manufacturer's declaration**

Yes

No

Not Applicable

**Supporting evidence:**

## OTHER SECURITY CONSIDERATIONS – OTHR.2

### Description of provision

*The 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 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.

### Reference

Adapted from

1. IEC TR 80001-2-2:2012 Section 5.2

### Manufacturer's declaration

- Yes
- No
- Not Applicable

**Supporting evidence:**



## OTHER SECURITY CONSIDERATIONS – OTHR.3

### Description of provision

*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.*

### Intent of the Provision

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

### Minimum Requirements

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

### Supporting Evidence

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.

### Reference

Adapted from

1. Manufacturer Disclosure Statement for Medical Device Security (MDS2) CONN-1.2

### Manufacturer's declaration

Yes

No

Not Applicable

**Supporting evidence:**



# 10 LEVEL 3 – PENETRATION TESTING

## 10.1. OVERVIEW

The objective of this activity is to determine if the Device Under Test (DUT) is resistant to common attacks through penetration testing.

Devices that attain Level 3 should be capable of providing resistance against attacks conducted by a basic attacker on exposed interfaces.

Level 3 does not seek to assert that the medical device is resistant to all attacks. However, Level 3 should provide basic assurance that the device is adequate to ward off the commonly known and straightforward attacks against such devices.

There are 3 components within Level 3 – Penetration Testing:

- a. Declaration of Conformity to Level 2 – Enhanced Provisions: To ensure that devices meet the set of enhanced security requirements.
- b. Software Binary Analysis: To analyse the device’s software (device firmware and companion applications such as desktop or mobile applications) for malware, known vulnerabilities in third party libraries used, and for software weaknesses.
- c. Penetration Testing: To assert that the medical device is reasonably resistant to common attacks and to prove that there are no obvious or critical vulnerabilities.

## 10.2. DECLARATION OF CONFORMITY TO ENHANCED PROVISIONS

### Level 2 – Enhanced Provisions

The enhanced security requirements are defined within Section 9: Level 2 – Enhanced Provisions.

Manufacturers may use the “Manufacturer’s declaration’ section within each provision to indicate conformity and provide the relevant support evidence.

## 10.3. SOFTWARE BINARY ANALYSIS AND PENETRATION TESTING

For software binary analysis and penetration testing, manufacturers may engage a testing laboratory of choice to conduct the testing.

Manufacturers may refer to [Scheme Specifications](#) [2] and [Minimum Test Specifications](#) [3] for details on the recommended testing requirements.

# 11 LEVEL 4 – ADVANCED TESTING

## 11.1. OVERVIEW

The objective of this activity is to determine if the Device Under Test (DUT) is resistant to enhanced attacks through security evaluation.

Devices that pass Level 4 should be capable of providing resistance against enhanced attacks since the device has been tested at a more in-depth level.

Level 4 does not seek to assert that the medical device is resistant to all attacks.

There are 3 components within Level 4 – Advanced Testing:

- a. Declaration of Conformity to Level 2 – Enhanced Provisions
- b. Software Binary Analysis: To analyse the device’s software (device firmware and companion applications such as desktop or mobile applications) for malware, known vulnerabilities in third party libraries used, and for software weaknesses.
- c. Security Evaluation: To assert that the medical device is reasonably resistant to enhanced attacks and to prove that there are no obvious or critical vulnerabilities.

## 11.2. DECLARATION OF CONFORMITY TO ENHANCED PROVISIONS

Level 2 – Enhanced Provisions

The enhanced security requirements are defined within Section 9: Level 2 – Enhanced Provisions.

Manufacturers may use the “Manufacturer’s declaration’ section within each provision to indicate conformity and provide the relevant support evidence.

## 11.3. SOFTWARE BINARY ANALYSIS AND SECURITY EVALUATION

For software binary analysis and security evaluation, manufacturers may engage a testing laboratory of choice to conduct the testing.

Manufacturers may refer to [Scheme Specifications](#) [2] and [Minimum Test Specifications](#) [3] for details on the recommended testing requirements.

## 12 REFERENCES

1. Cyber Security Agency of Singapore, Cybersecurity Labelling Scheme for Medical Devices - CLS(MD) (csa.gov.sg)
2. Cyber Security Agency of Singapore, "CLS(MD) Publication #4 - Assessment Methodology," Version 0.3, October 2023.
3. Cyber Security Agency of Singapore, "CLS(MD) Publication #2 - Scheme Specifications," Version 0.5, October 2023.
4. Cyber Security Agency of Singapore, "CLS(MD) Publication #5 - Minimum Test Specifications and Methodology," Version 0.5, October 2023.
5. Manufacturer Disclosure Statement for Medical Device Security (MDS2), 2022
6. IEC/TR 80001-2-2:2012, Application of risk management for IT-networks incorporating medical devices, Part 2-2: Guidance for the communication of medical device security needs, risks and controls, 2012.
7. NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, 2013.
8. Cyber Security Agency of Singapore, CCC-SP-151-4 Cybersecurity Labelling Scheme for IoT – CLS(IoT) Publication No. 4, Version 1.0, September 2023.
9. Singapore Standards Council, TR67:2018, Technical Reference – Connected device security, 2018.



This work is licensed under CC BY-SA 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-sa/4.0/>