Cybersecurity Labelling Scheme

FOR MEDICAL DEVICES

BY CYBER SECURITY AGENCY OF SINGAPORE

Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)] Publication No. 2

Scheme Specifications

October 2023
Version 0.5

FOREWORD

The Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)] is part of efforts from the Ministry of Health (MOH), Cyber Security Agency of Singapore (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) under the ambit of the Cyber Security Agency of Singapore (CSA). The CLS(MD) is jointly owned by MOH and CSA.

AMENDMENT RECORD

Version	Date	Author	Changes
0.5	October 2023	Cyber Security Agency of Singapore	Draft

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

CONTENTS

INTRODUCTION

1.0.1 This document aims to provide an overview of Cybersecurity Labelling Scheme for Medical Device [CLS(MD)]. It outlines the four (4) cybersecurity levels, the assurance activities, and the expected deliverables of each of the levels.

1.0.2 The intended audience for this document is the manufacturers who are interested in getting their Medical Devices labelled under CLS(MD) and testing laboratories who are responsible for testing the medical devices in accordance to the requirements of the CLS(MD).

1.0.3 This document is organised in the following manner:

a. Chapter 1 provides a broad overview of the 4 cybersecurity levels of the CLS(MD).

b. Chapter 0 elaborates on Level 1 – Declaration of Conformity to Baseline Security Requirements. It lists the objective, requirements, and the acceptance criteria.

c. Chapter 3 elaborates on Level 2 – Declaration of Conformity to Enhanced Security Requirements. It lists the objective, requirements, and the acceptance criteria.

d. Chapter 4 elaborates on Level 3 – Declaration of Conformity to Enhanced Security Requirements, Software Binary Analysis, and Penetration Testing. It lists the requirements, penetration testing scope, pass criteria, and the test deliverables expected by CCC.

e. Chapter 5 elaborates on Level 4 – Declaration of Conformity to Enhanced Security Requirements, Software Binary Analysis, and Security Evaluation. It lists the requirements, security evaluation scope, pass criteria, and the test deliverables expected by CCC.

1.0.4 The following roles are commonly referred in this document:

1. **Manufacturer** of the Device Under Test (DUT)

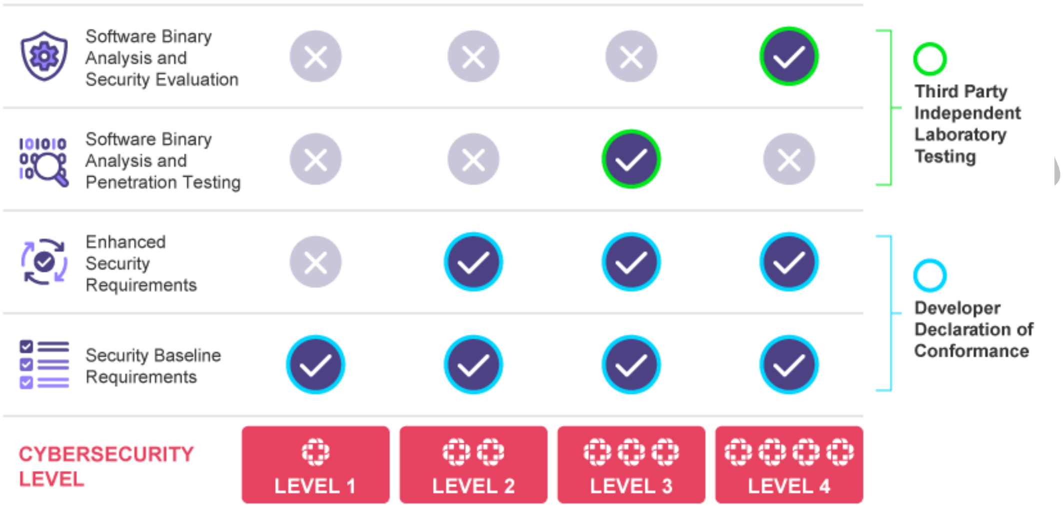
2. **Testing Laboratory (TL)** that performs the Penetration Testing for Level 3 or Security Evaluation for Level 4

3. **Cybersecurity Certification Centre (CCC)** that oversees the CLS(MD).

1 OVERVIEW

1.1 CYBERSECURITY LABELING SCHEME (CLS)

1.1.1 The following table provides an overview of the broad requirements for each labelling level of the CLS.



Software Binary Analysis and Security Evaluation	✕	✕	✕	✓	○ Third Party Independent Laboratory Testing
Software Binary Analysis and Penetration Testing	✕	✕	✓	✕	
Enhanced Security Requirements	✕	✓	✓	✓	○ Developer Declaration of Conformance
Security Baseline Requirements	✓	✓	✓	✓	
CYBERSECURITY LEVEL	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	

Figure 1 - CLS(MD) Overview

2 LEVEL 1 – BASELINE SECURITY REQUIREMENTS

2.1 OBJECTIVE

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

2.1.2 **Level 1 is based solely on <u>declaration of conformity</u> by the Manufacturer**.

2.1.3 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.

2.2 REQUIREMENTS

2.2.1 Level 1 consists of a baseline set of security requirements comprising of 6 requirements from both HSA – Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach [1] and the ANSI/NEMA HN 1-2019 - Manufacturer Disclosure Statement for Medical Device Security (MDS2) [2]. These requirements are documented within CLS(MD) Publication #4 - Assessment Methodology" [3].

2.2.2 The manufacturer shall declare conformity against the baseline security requirements.

2.3 DECLARATION OF CONFORMITY

2.3.1 Manufacturers are required to complete and submit the following to declare conformity to the security requirements:

- Declaration of Conformity
- Required supporting evidence.

2.3.2 The manufacturer shall refer to the "CLS(MD) Publication #4 - Assessment Methodology" [3] for details on the passing criteria and the expected supporting evidence required for each of the security requirement. The supporting evidence shall seek to enable the CCC to determine that the security requirements are met.

2.3.3 The supporting evidence can be provided in the following forms:

- In the entirety of the related documentation, with specific reference to the actual chapter/section/paragraph containing the required supporting evidence to substantiate the claim to the meeting of the requirement.

- As screen captures or snippets of the actual document where the snippets shall contain the required supporting evidence to substantiate the claim to the meeting of the requirement.

2.4 ACCEPTANCE CRITERIA

2.4.1 No independent testing by the testing laboratory is required for this level.

2.4.2 However, CCC will review the submitted Declaration of Conformity and supporting evidence. CLS(MD) Level 1 is only considered satisfied when CCC gains assurance through the submitted supporting evidence that the requirements are met.

2.4.3 Where necessary, CCC may choose to request for further clarifications and request a presentation from the manufacturer.

2.4.4 In the event of non-conformities, the manufacturer may choose to resolve them, or the application shall be considered as unsuccessful for Level 1.

2.4.5 Should any false declarations be subsequently discovered (possibly by the TL in subsequent testing or by other means), CCC reserves the full rights to enforce actions as described in Chapter 12 of CLS(MD) Publication #1 – Overview of the Scheme [4].

3 LEVEL 2 – ENHANCED SECURITY REQUIREMENTS

3.1 OBJECTIVE

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

3.1.2 **Level 2 is based solely on declaration of conformity by the manufacturer**.

3.1.3 Devices that have completed Level 2 would entail that the manufacturer has met a set of enhanced security requirements.

3.2 REQUIREMENTS

3.2.1 Level 2 consists of a set of 38 security requirements selected from the HSA – Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach [1], and the ANSI/NEMA HN 1-2019 - Manufacturer Disclosure Statement for Medical Device Security (MDS2) [2]. These requirements are documented within CLS(MD) Publication #4 - Assessment Methodology" [3].

3.2.2 The manufacturer shall meet all enhanced security requirements as stated within the Declaration of Conformity.

3.3 DECLARATION OF CONFORMITY

3.3.1 Manufacturers are required to complete and submit the following to declare conformity to the security requirements:

- Declaration of Conformity
- Required supporting evidence.

3.3.2 The manufacturer shall refer to the "CLS(MD) Publication #4 - Assessment Methodology" [3] for details on the passing criteria and the expected supporting evidence required for each of the security requirement. The supporting evidence shall seek to enable the CCC to determine that the security requirements are met.

3.3.3 The supporting evidence can be provided in the following forms:

- In the entirety of the related documentation, with specific reference to the actual chapter/section/paragraph which contains the required supporting evidence to substantiate the claim to the meeting of the requirement.
- As screen captures or snippets of the actual document where the snippets shall contain the required supporting evidence to substantiate the claim to the meeting of the requirement.

3.4 ACCEPTANCE CRITERIA

3.4.1 No independent testing by the testing laboratory is required for this level.

3.4.2 However, CCC will review the submitted Declaration of Conformity and supporting evidence. CLS(MD) Level 2 is only considered satisfied when CCC gains assurance through the submitted supporting evidence that the requirements are met.

3.4.3 Where necessary, CCC may choose to request for further clarifications and request a presentation from the manufacturer.

3.4.4 In the event of non-conformities, the manufacturer may choose to resolve them, or the application shall be considered as unsuccessful for Level 2.

3.4.5 Should any false declarations be subsequently discovered (possibly by the TL in subsequent testing or by other means), CCC reserves the full rights to enforce actions as described in Chapter 12 of CLS(MD) Publication #1 – Overview of the Scheme [4].

4 LEVEL 3 – ENHANCED SECURITY REQUIREMENTS, SOFTWARE BINARY ANALYSIS, AND PENETRATION TESTING

4.1 OBJECTIVE

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

4.1.2 There are three (3) main components for Level 3:

1. Declaration of Conformity to Enhanced Security Requirements.
2. Software Binary Analysis. The testing laboratory shall determine if the firmware and companion application(s) of the Device Under Test (DUT) are free from common software errors such as buffer overflown, known vulnerabilities in any of the third-party libraries being used, and known malware.
3. Penetration Testing. The testing laboratory shall determine if the devices is resistant against attacks conducted by a basic attacker.

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

4.1.4 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.

4.2 PRE-REQUISITES

4.2.1 Manufacturers are required to complete and submit the following to CCC to declare conformity to the security requirements:

- Declaration of Conformity
- Required supporting evidence.

4.2.2 The manufacturer shall provide the following to the testing laboratory:

- Firmware and companion applications
- Guidance document (installation/operation guide)
- Sufficient number of DUT to meet testing laboratory's requirements.

4.2.3 Guidance documents refers to written material such as service manuals, operator manuals, installation guides, etc., which is intended to be used by the user either operating, maintaining, or setting up the device to a secure state.

4.2.4 The manufacturer may be requested to provide a single unit of the DUT to the CCC. In the event of reports of security vulnerabilities for the DUT after the completion of the project, CCC may conduct internal investigations using the provided DUT.

4.3 ENHANCED SECURITY REQUIREMENTS

4.3.1 Level 3 includes requirements for Level 2 - Declaration of Conformity to Enhanced Security Requirements which is defined within Chapter 3 of this document.

4.4 SOFTWARE BINARY ANALYSIS

4.4.1 Software Binary Analysis comprises the following activities:

No.	Activities
1	Software Errors
2	Vulnerabilities in third party libraries/components, and hard-coded sensitive security parameters
3	Malware Scan
4	Mobile Application Scan
5	Search for Vulnerabilities in the Public Domain

4.4.2 The manufacturer shall provide the firmware binary and the companion applications (if available) of the DUT to the testing laboratory.

4.4.3 To facilitate testing, the firmware binary and companion applications must be provided in a format that is supported by the binary scanners (e.g., unencrypted, specific file extension, etc.). The manufacturer shall exercise due diligence to scan and remove any malwares before submission.

4.4.4 The manufacturer shall provide a Software Bill of Materials (SBOM) containing all software components (e.g., Micro_Httpd, OpenSSL, etc.) used in the DUT's firmware and companion applications (software applications, iOS mobile applications, Android mobile applications, etc.).

4.4.5 In addition, the hash values (SHA-256) of all firmware binary files and companion applications submitted shall be provided.

4.4.6 On the receipt of the binary files, the testing laboratory shall proceed to perform the binary scans using a suite of binary analysis tools.

4.4.7 The generated binary analyser reports shall be analysed by the testing laboratory.

4.4.8 The required binary analysis tools are available at the National Integrated Centre for Evaluation (NiCE). More information on NiCE is available at https://www.ntu.edu.sg/nice.

4.4.9 It is expected that the testing laboratory shall take a median of 3 to 5 man-days for the performance of the software binary analysis and the review of the test results alongside the manufacturer's method of resolution or justification.

Software Errors

4.4.10 The Binary Code Analysis tool is used to identify common software flaws such as buffer overflows. It is expected that there can be multiple false positives in the test results. The testing laboratory, together with the manufacturer, is expected to evaluate all relevant findings.

4.4.11 For all findings returned by the binary code analysis tool, the manufacturer shall perform an analysis if the findings are true positives or false positives.

4.4.12 For true positives, the manufacturer shall provide a method of resolution. The methods of resolution, not limited to the following:

- Perform a flaw remediation to address the discovered vulnerability.
- The vulnerability is assessed to be not exploitable for the DUT given the operational environment.

4.4.13 The manufacturer must apply remediation procedures for positive findings. Following remediation procedures, the testing laboratory shall re-test the binary code. The remediated findings and the remediation steps must be included in the report to CCC.

4.4.14 For false positives, the manufacturer shall provide a justification explaining why the finding is a false positive.

4.4.15 The manufacturer shall provide the analysis for both positive and false positives findings to the testing laboratory. The testing laboratory shall review the manufacturer's analysis and determine that the method of resolution or rationale for each finding is appropriate.

4.4.16 The testing laboratory shall submit a report including the following to CCC:

- List of true positives and the method of resolution taken by the manufacturer for each of the findings.
- List of false positives and the manufacturer's rationale for each of the finding on why it is a false positive.
- Testing laboratory's assessment on the manufacturer's method of resolution or rationale for each of the finding.

Vulnerabilities in third party libraries/components, and hard-coded sensitive security parameters

4.4.17 A Software Composition analyser is used to identify the usage of any third-party libraries and for such libraries, whether any known vulnerabilities (CVEs) are reported. The Software Composition analyser may also discover any hard-coded sensitive security parameters.

4.4.18 If the manufacturer has successfully implemented the development process requirements as specified within Level 2, it is expected that the list of findings reported by the Software Composition Analyser should be minimal, with most of the findings being remediated or accounted for.

4.4.19 Nonetheless, in some unexpected situations, the list of identified vulnerabilities might remain significant. For such situations, the manufacturer is strongly encouraged to withdraw the application and focus on remediating the flaws, rather than incurring unnecessary cost to proceed with the application process.

4.4.20 It is expected that the manufacturer shall provide the rationale and method of resolution taken to address all CVEs reported by the tool. The rationale and method of resolution taken shall be provided to the testing laboratory. Using the provided rationale and resolution, the testing laboratory shall make an assessment to determine that all CVEs reported are addressed and that the method of resolution taken by the manufacturer is sound and sufficient to address the CVE.

4.4.21 The method of resolution could be any, but not limited to, the following:

- Perform a flaw remediation to address the discovered vulnerability. Examples of flaw remediation could be the patching of vulnerable components to address vulnerabilities, disabling vulnerable components, implementing technical measures to address vulnerabilities.
- If the discovered vulnerability is a false positive (e.g., the vulnerable component is not being used), the manufacturer shall provide this assessment to the laboratory. The testing laboratory shall verify the suitability of this assessment and note it in the test report.
- Assess the vulnerability to be difficult/unexploitable. The assessment shall be provided to the testing laboratory and the testing laboratory will perform the first review of the suitability of this assessment.

4.4.22 It is also expected that the tool may not be able to detect all third-party libraries/components used in the firmware. Therefore, the testing laboratory shall identify libraries/components which are not detected by the tool by comparing the tool results against the Software Bill of Material provided by the manufacturer. The lab shall perform analysis to ensure that these libraries/components do not contain any known vulnerabilities.

4.4.23 The testing laboratory shall assess that third-party libraries/components used by the firmware are compliant with respective license requirements (GNU General Public License, BSD license, MIT, Creative Commons, Apache, etc.).

4.4.24 The testing laboratory shall determine that the firmware and the companion application does not contain hard-coded critical security parameters.

4.4.25 The testing laboratory shall assess that there are no exploitable third-party libraries/components. If the vulnerabilities are deemed to be highly exploitable, the manufacturer is required to update the libraries/components to a version without vulnerabilities, or to implement a custom patch/fix to address the vulnerability. The testing laboratory shall re-test the binary code following manufacturer's remediation procedures. The remediated findings and its remediation steps must be included in the report to CCC.

4.4.26 For each false positive, the manufacturer shall provide sufficient justification on why the finding is a false positive. The justification shall be reviewed by the testing laboratory on its appropriateness.

Malware Scan

4.4.27 Manufacturer shall ensure that the binary files provided is free from known malware.

4.4.28 The testing laboratory shall subject the binary files to a commercial malware scanner that exists as a cloud solution for malware analysis. Therefore, the manufacturer shall consent to allowing the binary files to be uploaded to a commercial malware scanner for malware analysis. Alternatively, local offline malware scanner can be used, on the condition that the scanner is up to date with the latest definitions.

4.4.29 In the event that firmware and/or the companion mobile application tests positive for malware, the initial malware scan results shall be confirmed using a different malware scanner. If both malware scanners confirm that the binary file tests positive for malware, CCC reserves the right to take appropriate actions against the manufacturer.

Mobile Application Scan

4.4.30 Where a companion mobile app is available to facilitate the usage of the DUT, the companion mobile app shall be subjected to binary analysis. The testing laboratory shall prioritise their analysis of the companion mobile app on the following areas:

- Hardcoded credentials or critical security parameters;
- Exposure of sensitive information, for example via insecure storage or insecure communication channels;
- Potential intrusion to privacy for example whether the app requests for rights/permissions that it is deemed not to require such as to user's calendar or device's camera; or where data is sent out despite the user explicitly denying such request.

4.4.31 Mobile applications across available platforms such as Android and iOS shall be subjected to the binary analysis.

4.4.32 The findings shall be resolved or justified as appropriately.

<u>Testing Laboratory Deliverables</u>

4.4.33 The testing laboratory shall submit a report containing the following:

1. Verdict on the software errors
2. Verdict on the third-party library and hard-coded sensitive security parameters
3. Verdict on the mobile application scan (if applicable)
4. Results on the search for potential vulnerabilities in the public domain

4.4.34 If vulnerabilities are identified during testing, the testing laboratory shall describe the identified vulnerabilities in the report and state the method of resolution undertaken by the manufacturer.

4.4.35 During the course of testing, if the testing laboratory discovers any discrepancies or false declarations in the manufacturer's declaration of conformity to the Security Baseline Requirements, International Standards, or Lifecycle requirements, the testing laboratory is to provide the information to CCC, and CCC reserves the full rights to enforce actions as described in Chapter 9.7 of CLS(MD) Publication #1 – Overview of the Scheme [4].

<u>Pass Criteria for Software Binary Analysis</u>

4.4.36 The firmware and the companion mobile application shall be free from identified exploitable vulnerabilities using the binary analysers. For non-conformity, the manufacturer and the testing laboratory can choose to provide due justification to CCC which must be supported by the testing laboratory. The exception will be reviewed and accepted by CCC on a case-by-case basis.

4.5 PENETRATION TESTING

4.5.1 This activity comprises the following tasks:

No.	Tasks
1	Device setup and verification of guidance documents
2	Conformity Verification – verifying that the device indeed implemented the security measures that the manufacturer has declared and specified in the conformity checklist.
3	Scheme-mandated minimum test specifications
4	Search for potential vulnerabilities in the public domain

5	Vulnerability analysis and freeform penetration testing, devising test cases based on:
	a) Software binary results;
	b) Known threat vectors;
	c) The laboratory's expertise and experience.

5	Password cracking (if applicable)

Table 1 – Assessment Tier #4 tasks

4.5.2 The testing laboratory shall conduct the abovementioned tasks concurrently where possible by leveraging on multiple units of the device and it is expected that it should take a median of 20 man-days, inclusive of drafting the test report and exclusive of administrative project overheads and potential delays due to technical or application deficiencies.

4.5.3 Nonetheless, the testing laboratory is required to spend a minimum of 8 days on Freeform Penetration Testing. The objective of this freeform testing is to serve as a feedback loop for the continuous refinement of the minimum test specification so to align with the current threat landscape.

4.5.4 The manufacturer shall facilitate the testing by the testing laboratory. For example, by providing sufficient units of the devices to the testing laboratory and responding to queries. The manufacturer shall note that certain tests might render the device to be unusable (e.g., physically damaged).

Device setup and verification of guidance documents

4.5.5 The objective of analysing the guidance document provided alongside the DUT is to determine that the user guidance guides the user into setting up the device into a secure state, and does not mislead the user into installing, operating, or maintaining the DUT in an insecure manner, and to minimise the risk of human or other errors in operation that may affect the security of the DUT. It seeks to identify if the guidance documentation may be potentially unclear, misleading, or unreasonable, that may lead to the insecure usage of the device.

4.5.6 The guidance document (i.e., user manual, installation guide, operation guide, etc.) shall consist of clear steps that guides the end-user to install and operate the DUT in a secure manner. The guidance document shall be written in a manner that is easily understood by the typical user of the DUT. It can be assumed that the typical user has little to no knowledge of cybersecurity. If the DUT functions are configurable, the guidance document shall indicate secure values as appropriate. The guidance document shall also describe possible modes of operation of the DUT, their consequences and procedures for returning the DUT back into a secure configuration.

4.5.7 The testing laboratory shall examine the guidance document(s) provided to determine that the guidance document provided meets the requirements stated above.

Conformity Verification

4.5.8 As part of the application, the manufacturer is required to declare conformity against the security provisions and provide evidence and descriptions of how these requirements have been implemented by the device.

4.5.9 The testing laboratory shall examine that the security measures are indeed being implemented, and that the implementation is appropriate to fulfil to the requirements, either through verification or by testing the device.

Scheme-mandated Minimum Test Specifications

4.5.10 In order to ensure consistent penetration testing of connected products across different testing laboratories, minimum test specifications are defined.

4.5.11 The testing laboratory shall ensure that the test objectives in the test specifications are achieved prior to the conduct of independent vulnerability analysis and penetration testing.

4.5.12 The testing laboratory shall take reference from CLS(MD) Publication – Minimum Test Specifications and Methodology [5] for this task. Supplementary Minimum Test Specification may be available for selected categories of products. Where such supplementary minimum test specification is available, the testing laboratory is required to include the additional tests.

4.5.13 It is of CCC's intention that the test specifications shall be revised in the future to keep up with the evolving threat landscape.

Search for potential vulnerabilities in the public domain

4.5.14 The testing laboratory shall examine sources of information publicly available to identify potential vulnerabilities for the DUT.

4.5.15 The testing laboratory shall also examine sources of information publicly available to identify generic vulnerabilities (vulnerabilities discovered on similar DUT-type) that could potentially be applicable for the DUT and determine if they are applicable for the DUT.

4.5.16 The testing laboratory can make use of several established sources. Examples are Common Vulnerabilities and Exposures (CVE), and public search engines (e.g., Google).

4.5.17 The testing laboratory shall also examine sources of information publicly available to check for DUT source code, binary code, manufacturer-confidential data, DUT user credentials, or other information that may be available to a potential attacker. E.g., source code or DUT default administrator credentials hosted on GitHub.

Vulnerability Analysis

4.5.18 From information collected through the preceding search for potential vulnerabilities in the public domain and from the report of the binary analysis covered under the Software Binary Analysis, the manufacturer shall devise a list of potential security vulnerabilities and potential attack paths.

4.5.19 The testing laboratory may also make use of vulnerability scanning tools and techniques to identify potential vulnerabilities.

4.5.20 Malformed Input Testing (also known as fuzz testing) should be conducted to discover coding errors, security loopholes in the software of the DUT. It involves inputting massive amounts of random data to the DUT in an attempt to make it malfunction and discover potential flaws.

4.5.21 The testing laboratory shall make use of automated fuzzing software tools. Due to the limited time period, it is advised that the testing laboratory focus time and effort on interfaces that are deemed more critical.

4.5.22 It is expected that fuzz testing may result in device crashes which is different from an exploitable vulnerability. The manufacturer, together with the testing laboratory shall, to their best effort, attempt to perform analysis on the crashes to determine if the issues are potentially an exploitable vulnerability.

4.5.23 When devising attack scenarios, the operational environment in which the DUT is expected to be used should be taken into consideration.

4.5.24 The testing laboratory should identify sensitive assets that must be protected and devise attack scenarios to test that the sensitive assets are indeed adequately protected (e.g., sensitive and private user data must be encrypted, cryptographic keys, passwords etc.).

<u>Penetration Testing</u>

4.5.25 Prior to the beginning of any testing, the testing laboratory shall arrange a kick-off meeting with CCC and the manufacturer to discuss the test approach and test plan.

4.5.26 The testing laboratory shall prioritise the test cases to ensure the intended outcome of the labelling scheme could be achieved.

4.5.27 The testing laboratory is not expected to perform advanced attacks (e.g., laser injection, hardware side channel attacks). However, should such attacks be feasible within the timeframe of the testing or be practically executed by a potential attacker in the actual deployment environment, the testing laboratory shall execute such attacks on the DUT during testing.

<u>Password Cracking</u>

4.5.28 If the testing laboratory manages to obtain encrypted files containing sensitive credentials (user credentials, credentials to associated web services, etc.), the testing laboratory shall explore the brute-forcing of these files in an attempt to retrieve them.

4.6 PASS CRITERIA

4.6.1 The DUT is deemed pass if no critical or significant vulnerabilities are uncovered.

4.7 DELIVERABLES

4.7.1 The testing laboratory shall submit a concise test report containing the following:

1. Executive Summary
2. Verdict on the analysis of guidance document
3. Test results from tests in Minimum Test Specification.
    a. For test cases the DUT passes, an indicative statement by the lab would suffice.
    b. For test cases which the DUT failed, the lab shall record the detailed setup and procedure such that the results could be reproduced.
4. Results on the search for potential vulnerabilities in the public domain, including the list of search terms.
5. Test cases and results of the penetration testing. The test cases could be described in high level. Recording of detailed setup and procedures are required only for test cases which succeeded in exploiting the DUT.

4.7.2 The testing laboratory shall also arrange for a meeting with CCC to present the results.

4.7.3 The testing laboratory may be required to perform additional testing if CCC deems the testing performed to be inadequate.

4.7.4 During the course of testing, if the testing laboratory discovers any discrepancies or false declarations in the manufacturer's declaration of conformity to the Security Baseline Requirements, International Standards, or Lifecycle requirements, the testing laboratory is to provide the information to CCC, and CCC reserves the full rights to enforce actions as described in Chapter 9.7 of CLS(MD) Publication #1 – Overview of the Scheme [4].

5 LEVEL 4 – ENHANCED SECURITY REQUIREMENTS, SOFTWARE BINARY ANALYSIS, AND SECURITY EVALUATION

5.1 OBJECTIVE

5.1.1 The objective of this activity is to determine if the DUT is resistant to enhanced attacks through security evaluation.

5.1.2 There are three (3) main components for Level 4:

1. Declaration of Conformity to Enhanced Security Requirements.
2. Software Binary Analysis. The testing laboratory shall determine if the firmware and companion mobile application of the Device Under Test (DUT) is free from common software errors such as buffer overflown, known vulnerabilities in any of the third-party libraries being used, and known malware.
3. Security Evaluation. The testing laboratory shall determine if the devices is resistant to enhanced attacks.

5.1.3 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.

5.1.4 The security evaluation does not seek to assert that the DUT is resistant to all attacks.

5.2 PRE-REQUISITES

5.2.1 The manufacturer shall provide the following to the testing laboratory:

1. Completed Conformity Checklist and Supporting Evidence
2. Firmware and Companion Applications
3. Guidance document (installation/operation guide)
4. Sufficient number of DUT to meet testing laboratory’s requirements
5. Device security design documentation

5.2.2 Guidance documents refers to written material such as service manuals, operator manuals, installation guides, etc. which is intended to be used by the user either operating, maintaining, or setting up the device.

5.2.3 The DUTs may be destroyed at the end of the evaluation.

5.2.4 The manufacturer shall provide a single unit of the DUT to CCC. In the event of reports of security vulnerabilities for the DUT after the completion of the project, CCC may conduct internal investigations using the provided DUT.

5.3 ENHANCED SECURITY REQUIREMENTS

5.3.1 Level 4 includes requirements from Level 2 – 'Declaration of Conformity to Enhanced Security Requirements' which is defined within Chapter 3 of this document.

5.4 SOFTWARE BINARY ANALYSIS

5.4.1 Level 4 includes requirements on Software Binary Analysis from Level 3, which is defined within Chapter 4.4 of this document.

5.5 SECURITY EVALUATION

5.5.1 The testing laboratory shall conduct a security evaluation on the medical device. The testing laboratory shall analyse security design documentation for the purposes of determining design weaknesses, to gain deeper understanding of how the security functionalities are implemented, with the objective of devising targeted test cases.

5.5.2 This activity comprises the following tasks:

No.	Tasks
1	Device setup and verification of guidance documents
2	Conformity Verification – verifying that the device indeed implemented the security measures that the manufacturer has declared and specified in the conformity checklist.
3	Scheme-mandated minimum test specifications
4	Analysis of Design Documentation
5	Search for potential vulnerabilities in the public domain
6	Static Code Analysis
7	Cryptographic Correctness Test

8	Vulnerability analysis and freeform penetration testing, devising test cases based on:
	d) The report from Assessment Tier #3;
	e) Known threat vectors;
	f) The laboratory's expertise and experience.

9	Password cracking (if applicable)

5.5.3 The testing laboratory shall conduct the abovementioned tasks concurrently where possible by leveraging on multiple units of the device and it is expected that it should take no longer than a median of 60 man-days, inclusive of drafting the test report and exclusive of administrative project overheads and potential delays due to technical or application deficiencies.

5.5.4 The manufacturer shall facilitate the testing by the testing laboratory. For example, by providing sufficient units of the devices to the testing laboratory and responding to queries. The manufacturer shall note that certain tests might render the device to be unusable (e.g., physically damaged).

Device setup and verification of guidance documents

5.5.5 The objective of analysing the guidance document provided alongside the DUT is to determine that the user guidance guides the user into setting up the device into a secure state, and does not mislead the user into installing, operating, or maintaining the DUT in an insecure manner, and to minimise the risk of human or other errors in operation that may affect the security of the DUT. It seeks to identify if the guidance documentation may be potentially unclear, misleading, or unreasonable, that may lead to the insecure usage of the device.

5.5.6 The guidance document (i.e., user manual, installation guide, operation guide, etc.) shall consist of clear steps that guides the end-user to install and operate the DUT in a secure manner. The guidance document shall be written in a manner that is easily understood by the typical user of the DUT. It can be assumed that the typical user has little to no knowledge of cybersecurity. If the DUT functions are configurable, the guidance document shall indicate secure values as appropriate. The guidance document shall also describe possible modes of operation of the DUT, their consequences and procedures for returning the DUT back into a secure configuration.

5.5.7 The testing laboratory shall examine the guidance document(s) provided to determine that the guidance document provided meets the requirements stated above.

Conformity Verification

5.5.8 As part of the application, the manufacturer is required to declare conformity against the security provisions and provide evidence and descriptions of how these requirements have been implemented by the device.

5.5.9 The testing laboratory shall examine that the security measures are indeed being implemented, and that the implementation is appropriate to fulfil to the requirements, either through verification or by testing the device.

Scheme-mandated Minimum Test Specifications

5.5.10 In order to ensure consistent penetration testing of connected products across different testing laboratories, minimum test specifications are defined.

5.5.11 The testing laboratory shall ensure that the test objectives in the test specifications are achieved prior to the conduct of independent vulnerability analysis and penetration testing.

5.5.12 The testing laboratory shall take reference from CLS(MD) Publication – Minimum Test Specifications and Methodology [5] for this task. Supplementary Minimum Test Specification may be available for selected categories of products. Where such supplementary minimum test specification is available, the testing laboratory is required to include the additional tests.

5.5.13 It is of CCC's intention that the test specifications shall be revised in the future to keep up with the evolving threat landscape.

Analysis of Design Documentation

5.5.14 The manufacturer shall provide design documentation containing the following information to the testing laboratory so that the security evaluator may gain an increased understanding of the device's security and design.

i. Architecture Overview. The Architecture Overview shall describe the operating system used; the software components used (a list of all libraries used).
   a. The Architecture Overview shall also describe how the device provides domain separation, self-protection and non-bypassability of security functionalities.

ii. Input Interfaces Specification. A description of the input interfaces available on the device, method of use, accepted parameters, input validation strategy, error messages). Examples of input interfaces include APIs, network protocol interfaces, system configuration parameters, etc.

iii. Security Functionality Input Interfaces. For each of the security functionality provided by the device, the manufacturer shall provide a description of the corresponding input interface describing its method of use, accepted parameters, input validation strategy on the interfaces, and error messages.

iv. Security Functionality Design Documentation. For all security functionality provided by the device (Secure Initialisation, Secure Storage, Secure Communications, Secure Updates, Identification and Authentication, Device Auditing/Logging, Secure Erasure, etc.), the manufacturer shall provide documentation describing how the security functionality is implemented.

v. Logical Flow and Interactions between security functionalities. The manufacturer shall provide documentation containing the logical flow and interactions between the different security functionalities of the device during its intended usage.

vi. Cryptography Specification describing the following:
   a. Cryptographic libraries
   b. Cryptographic protocols and algorithms used, the purpose, and the referenced standard for the protocols and algorithms.
   c. Cryptographic key sizes in bits
   d. Cryptographic key management process (key generation, key distribution, key storage, key access, key derivation, key destruction)
   e. Hierarchical relation between the cryptographic keys
   f. Random number generation (RNG). Description of random number generator used (Physical, non-physical true, deterministic, hybrid physical, hybrid deterministic random

number generator), the standard the RNG conforms to and the expected output of the RNG.

g. Details of the cryptographic correctness tests performed for the device and their corresponding results. Cryptographic protocols can be tested by communicating with an independent known-good implementation, and cryptographic algorithms can be tested using randomly generated known-answer tests, with test vectors being generated or verified by an independent, known-good implementation.

5.5.15 The design documentation shall be of sufficient level of technical detail such that the testing laboratory is able to gain a thorough level of understanding of the security functionality implementation for the purposes of vulnerability analysis.

5.5.16 The testing laboratory is not expected to provide a summary on the sufficiency of the documentation. However, the testing laboratory should seek to provide a brief overview of the security implementation adopted in the medical device.

5.5.17 If parts of the device relevant for the security evaluation are provided by third parties or if the manufacturer does not hold the rights to the part relevant, the manufacturer shall ensure that the third party(s)'s cooperation and participation in the procedure is ensured. For example, where a certain portion of the device has been purchased and the manufacturer does not have the rights to the design documentation of this portion of the device for the purposes of the evaluation.

Search for potential vulnerabilities in the public domain

5.5.18 The testing laboratory shall examine sources of information publicly available to identify potential vulnerabilities for the DUT.

5.5.19 The testing laboratory shall also examine sources of information publicly available to identify generic vulnerabilities (vulnerabilities discovered on similar DUT-type) that could potentially be applicable for the DUT and determine if they are applicable for the DUT.

5.5.20 The testing laboratory can make use of several established sources. Examples are Common Vulnerabilities and Exposures (CVE), and public search engines (e.g., Google).

5.5.21 The testing laboratory shall also examine sources of information publicly available to check for DUT source code, binary code, manufacturer-confidential data, DUT user credentials, or other information that may be available to a potential attacker. E.g., source code or DUT default administrator credentials hosted on GitHub.

Static Code Analysis

5.5.22 The manufacturer shall perform static code analysis using well-known static code analysers on source code related to security functionality and provide the results of the static code analysis to the testing laboratory.

5.5.23 The testing laboratory shall perform an analysis of the results to determine if the source code is free of software vulnerabilities.

5.5.24 If the manufacturer has successfully implemented the development process requirements specified in Level 2, it is expected that the list of findings reported by the Static Code Analyser should be minimal.

5.5.25 Nonetheless, in some unexpected situations, the list of identified vulnerabilities might remain significant. For such situations, the manufacturer is strongly encouraged to withdraw the application and focus on remediating the flaws, rather than incurring unnecessary cost to proceed with the application process.

5.5.26 It is expected that the manufacturer shall provide the rationale and remediation taken to address each software vulnerability found. The rationale and remediation shall be provided to the testing laboratory.

5.5.27 The method of resolution could be any, but not limited to, the following:

- Perform a flaw remediation to address the discovered vulnerability. Examples of flaw remediation could be the patching of vulnerable components to address vulnerabilities, disabling vulnerable components, implementing technical measures to address vulnerabilities.
- If the discovered vulnerability is a false positive (e.g., the vulnerable component is not being used), the manufacturer shall provide this assessment to the laboratory. The testing laboratory shall verify the suitability of this assessment and note it in the test report.
- Assess the vulnerability to be difficult/unexploitable. The assessment shall be provided to the testing laboratory and the testing laboratory will perform the first review of the suitability of this assessment.

5.5.28 In the scenario where the static code analysis results suggests that the source code for certain related to security functionality are showing signs of vulnerabilities and that the static code analyser's results are insufficient, the testing laboratory may request access to the particular source code of interest for further in-depth source code review.

5.5.29 In the event that the lab determines that certain parts of the source code related to security functionality are vulnerable and that the vulnerabilities are not sufficiently mitigated, CCC reserves the right to require that the relevant source code be provided for CCC's assessment.

Cryptographic Correctness Test

5.5.30 The testing laboratory shall perform a review of the cryptographic specification to determine that the cryptographic mechanisms used are suitable to meet the security objectives the device or usage scenario requires, and perform cryptographic correctness tests on all cryptographic protocols/algorithms used by the device.

5.5.31 The testing laboratory shall test the utilised cryptographic protocols by communicating with an independent known-good implementation, and test the utilised cryptographic algorithms via the use of randomly generated known-answer tests, with test vectors being generated or verified by an independent, known-good implementation.

Vulnerability Analysis

5.5.32 From information collected through the preceding search for potential vulnerabilities in the public domain, report of the binary analysis covered during Software Binary Analysis, and design documentation, the manufacturer shall devise a list of potential security vulnerabilities and potential attack paths.

5.5.33 The testing laboratory may make use of vulnerability scanning tools and techniques to identify potential vulnerabilities.

5.5.34 Malformed Input Testing (also known as fuzz testing) should be conducted to discover coding errors, security loopholes in the software of the DUT. It involves inputting massive amounts of random data to the DUT in an attempt to make it malfunction and discover potential flaws.

5.5.35 The testing laboratory shall make use of automated fuzzing software tools. Due to the limited time period, it is advised that the testing laboratory focus time and effort on interfaces that are deemed more critical.

5.5.36 It is expected that fuzz testing may result in device crashes which is different from an exploitable vulnerability. The manufacturer, together with the testing laboratory shall, to their best effort, attempt to perform analysis on the crashes to determine if the issues are potentially an exploitable vulnerability.

5.5.37 When devising attack scenarios, the operational environment in which the DUT is expected to be used should be taken into consideration.

5.5.38 The testing laboratory should identify sensitive assets that must be protected and devise attack scenarios to test that the sensitive assets are indeed adequately protected (e.g., Sensitive and private user data must be encrypted, cryptographic keys, passwords etc.).

Conduct of Penetration Testing

5.5.39 Following the vulnerability analysis performed, the testing laboratory shall devise targeted test cases for the purpose of penetration testing.

Password Cracking

5.5.40 If the testing laboratory manages to obtain encrypted files containing sensitive credentials (user credentials, credentials to associated web services, etc.), the testing laboratory shall explore the brute-forcing of these files in an attempt to retrieve them.

5.6 PASS CRITERIA

5.6.1 The DUT is deemed pass if no critical or significant vulnerabilities are uncovered.

5.7 DELIVERABLES

5.7.1 Prior to the beginning of any testing, the testing laboratory shall arrange a kick-off meeting with CCC and the manufacturer to discuss the test approach and test plan.

5.7.2 After the conclusion of testing, the testing laboratory shall submit an evaluation report containing the following:

1. Executive Summary
2. Brief overview on the security implementation on the medical device
3. Results from the Software Binary Analysis
4. Verdict on the analysis of guidance document
5. Results on the Conformity Verification
6. Test results from tests in Minimum Test Specification.
7. Results on the search for potential vulnerabilities in the public domain, including the list of search terms.
8. Test results from Static Code Analysis
9. Test results on the Cryptographic Correctness Test.
10. Summary of the Vulnerability Analysis performed.
11. Summary of the Security Evaluation performed.

5.7.3 The report should include test cases and its corresponding results. The test cases could be described in high level. For test cases the DUT passes, an indicative statement by the lab would suffice. Recording of detailed setup and procedures are required only for test cases which succeeded in the exploitation of the DUT.

5.7.4 The testing laboratory shall arrange for a meeting with CCC to present the results.

5.7.5 The testing laboratory may be required to perform additional testing if CCC deems the testing performed to be inadequate.

5.7.6 During the course of testing, if the testing laboratory discovers any discrepancies or false declarations in the manufacturer's declaration of conformity to the Security Baseline Requirements, International Standards, or Lifecycle requirements, the testing laboratory is to provide the information to CCC, CCC reserves the full rights to enforce actions as described in Chapter 9.7 of CLS(MD) Publication #1 – Overview of the Scheme [4].

REFERENCES

[1] Health Sciences Authority, "Regulatory Guidelines for Software Medical Devices - A Life Cycle Approach," Revision 2.0, April 2022.

[2] National Electrical Manufacturers Association, "Manufacturer Disclosure Statement for Medical Device Security (MDS2)".

[3] Cyber Security Agency of Singapore, "CLS(MD) Publication #4 - Assessment Methodology," Version 0.3, October 2023.

[4] Cyber Security Agency of Singapore, "CLS(MD) Publication #1 - Overview of CLS(MD)," Version 0.5, October 2023.

[5] Cyber Security Agency of Singapore, "CLS(MD) Publication #5 - Minimum Test Specifications and Methodology," Version 0.5, October 2023.

ACRONYMS

The following acronyms are used in CLS Publication 1, 2 and 3:

CCC	Cybersecurity Certification Centre
CSA	Cyber Security Agency of Singapore
DUT	Device Under Test
HPL	Historical Product List
LPL	Labelled Product List
TL	Testing Laboratory