Industry Consultation on the Proposed Cybersecurity Labelling Scheme for Medical Devices, CLS(MD)

Issued by Ministry of Health (MOH), Cyber Security Agency of Singapore (CSA), Health Sciences Authority (HSA), and Integrated Health Information Systems (IHiS)

25 January 2023

Content

Industry Consultation on the Proposed Cybersecurity Labelling Scheme for Medical Devices, CLS(MD)

Industry Consultation on the Proposed Cybersecurity Labelling Scheme for Medical Devices, CLS(MD)

1. Objective

The Ministry of Health (MOH), Cyber Security Agency of Singapore (CSA), Health Sciences Authority (HSA), and Integrated Health Information Systems (IHiS) would like to invite feedback and comments from our stakeholders on the proposed Cybersecurity Labelling Scheme for Medical Devices [CLS(MD)].

2. This document is intended to provide the details on the proposed approach and requirements for CLS(MD).

2. Scope

3. This document applies to all Medical Devices as described in the First Schedule of the Health Products Act (Cap122D, 2008 Rev Ed)[1] **and** have any of the following characteristics:

i. Handles personal identifiable information (PII) and clinical data and has the ability to collect, store, process, or transfer such data;

ii. Connects to other devices, systems, and services - Has the ability to communicate using wired and / or wireless communication protocols through a network of connections.

3. Definitions

4. **"Qualified Practitioner"** (as set out in the Health Products (Medical Devices) Regulations) means:

i. A registered medical practitioner under the Medical Registration Act (Cap. 174), when acting in the course of providing medical treatment to a patient under his care; or

ii. A registered dentist under the Dental Registration Act (Cap. 76) whose name appears in the first division of the Register of Dentists maintained and kept under section 13(1)(a) of that Act, when acting in the course of providing dental treatment to a patient under his care.

5. **"Professional use only" medical device** (as set out in the Health Products (Medical Devices) Regulations) means a medical device that is to be used on an individual solely by, or under the supervision of, a qualified practitioner.

6. **"Developer"** means the manufacturer/developer of the Medical Device.

[1] https://sso.agc.gov.sg/SL-Supp/S320-2018/Published/20180525170000?DocDate=20180525170000#pr2-

4. Audience

7. Medical Device manufacturers/developers and local dealers/registrants.

5. Background

8. The use of medical devices has gained momentum over the years worldwide to improve patients' health and lower care costs. However, connection of devices to networks or the internet also exposes devices to increased cyber risks. The cost of healthcare breaches worldwide is among the highest, if not the highest, among all sectors[2].

9. The integrity of medical devices is important to patient safety on three levels. First, unauthorised tampering of these devices e.g. insulin dosage settings of insulin pumps or pacing rate of pacemakers can harm patients directly[3]. Second, the alteration of data could cause inappropriate treatment, thereby causing harm. Third, malicious activities spreading across corporate network either from the device or other entry points can cripple the entire healthcare IT network, thereby impacting patient care services beyond the affected healthcare facility.

10. To tackle this cyber-risk, HSA has rolled out and implemented cybersecurity guidelines since 2016[4]. Overseas jurisdictions are also starting to put in place regulatory measures to ensure minimum cybersecurity standards for medical devices. For example, the Therapeutic Goods Administration (TGA) in Australia issued pre- and post-market cybersecurity regulatory recommendations for medical devices on 8 April 2021 and updated them on 24 November 2022. The United States Food and Drug Administration (FDA) issued a new draft guidance on 8 April 2022 to further emphasise the importance of ensuring devices are designed securely, enabling cybersecurity risks to be mitigated throughout the lifecycle of the devices as well as outlining premarket submission to address cybersecurity concerns.

11. Learning from the experience of recent global reported cybersecurity incidents, such as ransomware attack on the electronic medical record system incident faced by Handa hospital in Tsurugi, Tokushima Prefecture[5] on 31 Oct 2021, and the rise of ransomware attacks on the United States hospitals[6], a pre-emptive approach to reduce the likelihood of a successful breach or, if it does happen, to reduce the impact, is critical.

12. Taking into consideration the increased connectivity and digitalisation of medical devices alongside the evolving threat landscape that could impact healthcare service delivery, the Cybersecurity Labelling Scheme for Medical Devices, CLS(MD) was created. This is a joint initiative by MOH, CSA, HSA, and IHiS, and envisions to **improve the visibility of medical devices security, raise overall cyber hygiene levels, and better secure Singapore's cyberspace** for both data protection and patient safety in our healthcare sector.

[2] https://www.healthcareitnews.com/news/healthcare-breach-costs-hit-record-high
[3] https://www.fda.gov/medical-devices/medical-device-recalls/medtronic-recalls-minimed-insulin-pumps-incorrect-insulin-dosing
[4] https://www.hsa.gov.sg/medical-devices/guidance-documents
[5] https://www.japantimes.co.jp/news/2022/01/24/national/ransomware-attack-hospital-server
[6] https://www.theguardian.com/technology/2022/jul/14/ransomware-attacks-cybersecurity-targeting-us-hospitals

13. In determining the scheme, local[7] and international policies, and guidelines are reviewed. This is to ensure that (i) the industry is familiar to what would be imposed; (ii) existing policies are harmonised, and (iii) the final set of requirements will be validated.

14. Under the scheme, medical devices, as defined in para 3 will be rated according to their levels of cybersecurity provisions. It aims to improve security awareness by making such provisions more transparent to the general public and healthcare providers, thereby enabling them to identify products with the appropriate cybersecurity provisions and subsequently make informed purchasing decisions.

15. Other than Level 1, which is already required for HSA's product registration and market availability, all other levels in the framework are, in-principle, voluntary. However, given the increasing cybersecurity threats, requirements may increasingly be placed on ensuring the secure use of these medical devices.

6. Framework

16. The CLS(MD) comprises four (4) cybersecurity levels, with each higher level being more comprehensive in the assessment and requirements. Products that apply for the Cybersecurity Label shall undergo a series of assessments and tests, depending on the level that the developer wishes to attain. Owing to the progressive nature of the framework assessment, application to higher levels include the evaluation of requirements of the lower levels to be completed in sequence. Please refer to **Annex A** for the certification process details.

17. The requirements of testing under each of the cybersecurity levels are summarised in Figure 1 - Cybersecurity Assessment Levels below.

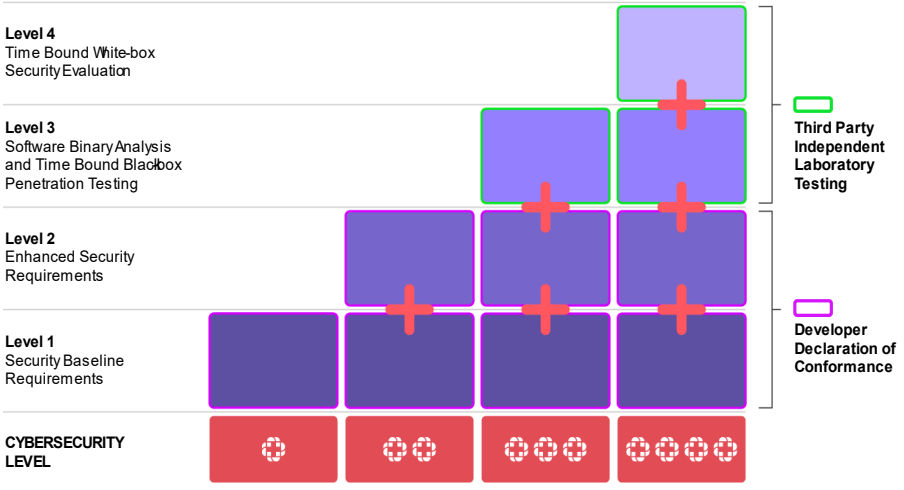

Figure 1 - Cybersecurity Assessment Levels

[7] https://www.hsa.gov.sg/medical-devices/guidance-documents

18. The CLS(MD) comprises 38 cybersecurity requirements (provided in **Annex B1 and B2**) specifying device lifecycle and capability cybersecurity requirements, software binary analysis, and penetration testing.

19. The 38 requirements are assigned into Levels 1 and 2 with consideration of the existing and upcoming policies in the healthcare sector.

6.1 Level 1 – Baseline Security Requirements

20. Level 1 – Baseline Security Requirements currently consists of four (4) cybersecurity requirements (Clauses 1, 7, 10, 20 in **Annex B1**) used by HSA in the review of medical devices seeking registration in Singapore. These requirements are internationally aligned and consist of establishing a cybersecurity risk management process to identify and mitigate all known and foreseeable vulnerabilities affecting the medical device and implement a systematic product maintenance process. This ensures that the emerging vulnerabilities are identified and evaluated on an on-going basis and effectively managed throughout the medical device lifecycle.

21. On top of the four existing requirements specified in para 20, the following two (2) clauses (Clauses 18 and 19 in **Annex B2**) are also being considered for inclusion into Level 1. This means that medical devices must also meet these two clauses in addition to HSA's current 4 cybersecurity requirements to qualify for CLS(MD) Level 1, which is required for registration and market entry. These two clauses are deemed as basic cybersecurity hygiene practice and are also requirements in the CLS scheme for IoT devices. Since medical devices should at least be held to the same, if not higher cybersecurity standards, these two clauses are deemed as important for CLS(MD) Level 1:

Clause	Provision	Supporting Evidence Requirements	Clause Intent
18	Where passwords are used and, in any state, other than the factory default, the **medical device passwords shall be unique per device or defined by the user**. Where pre-installed passwords are used, they shall be unique per device and sufficiently random.	Supporting evidence shall describe the following: 1. Does the device ship with factory default passwords that are universal across devices, with a pre-installed unique per device password, or does the device force the user to define a new password during initial setup? 2. If the device is shipped with a pre-installed unique per device password to avoid having universal default passwords, how are the pre-installed passwords generated for each device and what is done to ensure that the pre-installed passwords are sufficiently random? Are the randomised passwords based on any device information (MAC address, etc.)? The developer shall provide 5 instances of randomised passwords that are generated using the password randomisation mechanism. Minimally, the following are required for pre-installed passwords: 1. Passwords with incremental counters ("password1", "password2") are not allowed. 2. Pre-installed passwords must be sufficiently randomised using a random function. 3. Passwords must not be relatable in an	The objective of this clause is to ensure that the device **does not utilise a universal default password**. Utilising universal default passwords has been the source of security problems. If one device is compromised, all devices with that factory universal default password can be compromised. If the device comes with a universal default password, the device shall force the user to define a new password during initial setup. The requirement can also be met if the device is configured

		obvious manner to public information such as MAC address or Wi-Fi SSID. Please note that there are many mechanisms used for performing authentication, and passwords are not the only mechanism for authenticating a user to a device. If other authentication mechanisms are used, please provide details.	with pre-installed unique per device passwords. These passwords must be unique per device and sufficiently random, and not related in an obvious manner to public information (i.e. MAC Address, Wi-Fi SSID, etc.).
19	The device shall have a mechanism available which **makes brute force attacks on authentication mechanisms impractical**.	Supporting evidence shall show the mechanism(s) that can be used to change the authentication method reference value.	The objective of this clause is to ensure that the **device is not susceptible to brute force attacks on authentication mechanisms.** **In emergency situations, if the authentication rate limiting mechanism is triggered, the emergency break-glass feature can be used**. Refer to Clause 16 - 'The device shall support and enforce authentication for all users and roles. Exception is when the emergency access (i.e. physical break glass) is activated)'. This would allow the device to continue to operate in Safe Mode or Limited Mode (with limited capabilities sufficient for use in emergency operations). Some examples (non-exhaustive) of authentication rate limiting mechanisms: • Throttling mechanism which introduces a random delay between authentication attempts • Account lockouts after a defined number of incorrect attempts • CAPTCHA

			• IP Address blocking after multiple failed logins • Two-factor authentication

6.2 Level 2 – Enhanced Security Requirements

22. Level 2 – Enhanced Security Requirements is premised upon the developer's declaration of conformity to a set of cybersecurity requirements (consisting of the four clauses in Level 1 and the remaining 34 clauses **-** please refer to the **Annex B2** for the details of these additional clauses). The manufacturer shall complete and submit a declaration of conformity for the 38 security requirements. CSA shall review the declaration of conformity and supporting evidence prior to approval of Level 2 label.

6.3 Level 3 – Software Binary Analysis and Time-Bound Black-box Penetration Testing

23. Level 3 – Software Binary Analysis and Time-Bound Black-box Penetration Testing comprises the following components:

a. Declaration of Conformity to Security Requirements. The manufacturer shall complete and submit a declaration of conformity for the 38 cybersecurity requirements (clauses located in **Annex B1 and B2**). CSA shall review the declaration of conformity and supporting evidence prior to approval of Level 3 label.

b. Software Binary Analysis. The medical devices' software (firmware, companion mobile applications if any) will be analysed for **Common Vulnerabilities and Exposures (CVEs)** in third party libraries used, for malware, and for software weaknesses such as buffer overflow. The analysis will be performed with the aid of a combination of binary software composition analyser, malware scanner, and mobile application scanners. The scan results shall be reviewed and interpreted by the testing laboratory. At the end of this activity, the testing laboratory is expected to submit a report to CSA outlining the test results, identified issues, and corresponding method of resolutions to the issues.

c. Time-Bound Black-box Penetration Testing. A one-month time-bound black-box penetration testing by a testing laboratory is intended to **assert that the device is reasonably resistant to common attacks found applicable to medical devices, and to prove that there are no obvious or critical vulnerabilities**. Leveraging on basic tools and techniques as a trade-off for cost and effort, the penetration testing does not seek to assert that the medical device is resistant to all attacks. However, the penetration testing should provide basic assurance that the medical device is adequate to ward off the commonly known and straightforward attacks against such devices.

24. The black-box penetration testing shall consist of the following sub-activities:

a. Device setup and verification of guidance documents;
b. Conformity verification to ensure that the device has indeed implemented the security measures as declared and specified in the conformity checklist;

c. Scheme-mandated Minimum Test Specifications[8] (set of tests that must be performed and discussed with the developer);
d. Search for potential vulnerabilities in the public domain; and
e. Vulnerability Analysis and Freeform Penetration Testing, devising test cases based on the findings in the software binary analysis, known threat vectors, and the testing laboratory's expertise and experience.

25. To facilitate the black-box penetration testing, the applicant shall ensure that the following are provided to the testing laboratory:

a. Firmware and associated software applications required for device functions (if any);
b. Sufficient units of the medical devices as required by the testing laboratory; and
c. User guidance documents.

26. At the end of this activity, the testing laboratory is expected to submit a report to CSA outlining the test results, identified issues, and corresponding method of resolutions to the issues.

27. The report will be reviewed by CSA prior to approval of Level 3 label. The device is deemed to pass if no critical or significant vulnerabilities are uncovered.

6.4 Level 4 – Time Bound White-box Security Evaluation

28. Level 4 – Level 4 intends to reference the ETSI prEN17640 – Fixed time cybersecurity evaluation methodology as the basis, with additional components such as:

a. Declaration of Conformity to Security Requirements. The manufacturer shall complete and submit a declaration of conformity for the 38 cybersecurity requirements (clauses located in **Annex B1 and B2**). The manufacturer shall complete and submit a conformity checklist specifying conformity status to the security requirements. CSA shall review the declaration of conformity, rationale, and supporting evidence prior to approval of Level 4 label.

b. Software Binary Analysis. The medical devices' software (firmware, companion mobile applications if any) will be analysed for **CVEs** in third party libraries used, for malware, and for software weaknesses such as buffer overflow. The analysis will be performed with the aid of a combination of binary software composition analyser, malware scanner, and mobile application scanners. The scan results shall be reviewed and interpreted by the testing laboratory. At the end of this activity, the testing laboratory is expected to submit a report to CSA outlining the test results, identified issues, and corresponding method of resolutions to the issues.

c. The time-bound white-box security evaluation of the medical device will be performed by a testing laboratory. The three-month time-bound white-box security evaluation is **intended to provide a higher-level assurance**. The security evaluation seeks to determine whether the design of the medical device is fundamentally secure and whether the developer has implemented it securely. With greater knowledge on how the device is designed and implemented, more targeted test cases could be derived. The rigour with which the penetration testing is conducted will be more stringent and comprehensive, leveraging on more advanced

[8] This is a sample document of how the Minimum Test Specification (MTS) might look like. https://www.csa.gov.sg/-/media/Csa/Documents/CLS/PUB-CLS--Minimum-Test-Specification-v1-1.pdf

tools and sophisticated testing techniques. This would provide assurance to the users that medical device is capable to ward off commonly known and straightforward attacks, **as well as more moderately complex attacks against such devices.**

29. Examples of schemes that are based on fixed time security evaluation methodology include Germany's BSZ and France's CSPN. Germany's BSZ publishes a three-month fixed time for such a scheme.

30. The white-box security evaluation shall consist of the following sub-activities:

a. Device setup and verification of guidance documents;
b. Review of the product security design documents;
c. Conformity verification to ensure that the device has indeed implemented the security measures as declared and specified in the conformity checklist;
d. Scheme-mandated Minimum Test Specifications[9] (set of tests that must be performed and discussed with the developer);
e. Search for potential vulnerabilities in the public domain; and
f. Vulnerability Analysis and Freeform Penetration Testing, devising test cases based on the additional information on the design/implementation of the security functionalities and security architecture, findings in the software binary analysis, known threat vectors, and the testing laboratory's expertise and experience.

31. To facilitate the white-box security evaluation, the applicant shall ensure that the following are provided to the testing laboratory:

a. Sufficient units of the medical devices as required by the testing laboratory;
b. User guidance documents; and
c. Information on the design and implementation of the security functionalities.

32. At the end of this activity, the testing laboratory is expected to submit a report to CSA outlining the test results, identified issues, and corresponding method of resolutions to the issues.

33. The report will be reviewed by CSA prior to approval of Level 4 label. The device is deemed to pass if no critical or significant vulnerabilities are uncovered.

34. The duration for adequate black-box penetration testing and white-box security evaluation are recommended to be one month and three months respectively.

35. CSA considers ETSI prEN17640 as the underlying security evaluation methodology more suitable for CLS(MD) Level 4, compared to a more formalised certification scheme such as Common Criteria (ISO/IEC 15408).

7. Requirements for CLS(MD) Testing Laboratories

36. The testing laboratory performing the Level 3 and Level 4 evaluations shall meet the following requirements:

[9] https://www.csa.gov.sg/-/media/Csa/Documents/CLS/PUB-CLS--Minimum-Test-Specification-v1-1.pdf

i. ISO/IEC 17025. The testing laboratory shall be accredited or in the process of *accreditation (applicable for local laboratory only)* by the Singapore Accreditation Council (SAC)[10] or by other recognised Accreditation Bodies in accordance with the ISO/IEC 17025 for testing laboratories in the domain of IT/ICT/IoT security. The recognised Accreditation Body shall be a member of the International Accreditation Forum (IAF, https://www.iaf.nu/) and of the International Laboratory Accreditation Cooperation (ILAC, https://www.ilac.org/).

ii. Quality System. As part of ISO/IEC 17025 requirements, the testing laboratory shall have and comply with a quality system, which is documented in a quality manual, defining the testing laboratory's policies and objectives, roles and responsibilities for managerial and technical staff members and procedures for control of documents and records.

iii. Impartiality. If the testing laboratory is part of an organisation that performs activities other than security evaluations (e.g. consultation to the developer, developer, etc.), the testing laboratory shall identify actual and potential conflicts of interest and ensure clear separation of control to ensure that there is no undue influence on the testing activities. The testing laboratory shall be an independent evaluation laboratory, free of any undue commercial, financial and other interest of the medical device it would be testing.

iv. Environmental Conditions. The testing laboratory shall ensure that the environment in which it operates will not affect the correctness, reliability and confidentiality of the testing deliverables and results of the security testing and evaluation. For instance, access to and use of the testing laboratory premises must be controlled with effective separation of medical device security testing activities from other incompatible activities.

v. Methods. The testing laboratory shall use methodology that conforms to the requirements of the CLS(MD) and any other applicable international or regional standards. All methods, procedures or instructions used during testing shall be documented. The testing laboratory shall ensure that specialised tools used are identifiable, subject to specific configuration management, and for the testing and results to be reproducible. The testing laboratory shall retain all records relating to the testing, including records of original observations, derived data and other relevant information, to establish an audit trail.

vi. Security Policy. The testing laboratory shall have an appropriate security policy, preferably conforming to ISO/IEC 27001 and shall be able to meet the security requirements for handling protected information related to the evaluation of medical devices. The security policy shall set out to maintain the high degree of security required to protect commercially sensitive information, specifying procedures for human resources security, physical and environmental security, communications and operations management and access control preferably with reference to the ISO/IEC 27001/2 standard. For guidance on implementing information security controls, the evaluation laboratory may refer to ISO/IEC 27002.

vii. Technical Competency. The testing laboratory shall demonstrate to CSA that it is able to perform medical device security evaluations to the requirements of the scheme. The testing laboratory shall ensure the training needs of staff members are identified and provided for.

[10] The SAC is the National Accreditation Body for the independent accreditation of conformity assessment bodies in Singapore. More information regarding SAC is available at https://www.sac-accreditation.gov.sg/.

The staff members of the testing laboratory are expected to demonstrate their technical competency, either by proof of qualification, a written test, or other appropriate means.

37. The CLS(MD) requirements are subject to periodic review considering the rapidly changing cybersecurity landscape and advancements in technology.

8. CLS(MD) Labels

8.1 Proposed Design and Conditions of the Cybersecurity Label

38. Cybersecurity Labels will be issued by CSA for medical devices that meet the requirements in the CLS(MD) framework, including Level 1.

39. The proposed designs and sizes of the Cybersecurity Labels are below:

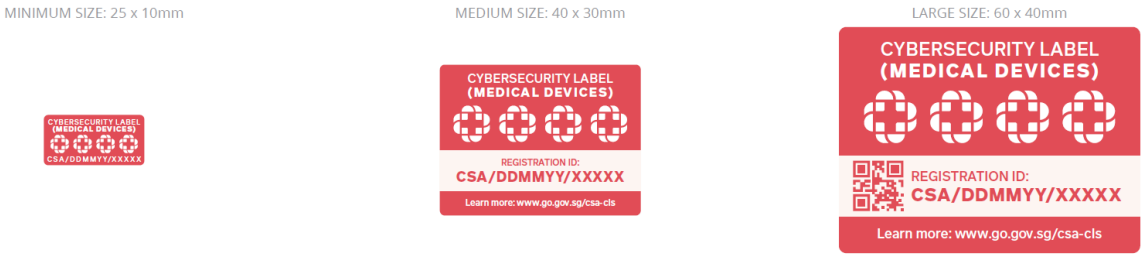

Figure 2- Sample Cybersecurity Labels

40. The label shall be affixed on the packaging of devices that can be sold to non-qualified practitioners. This is to increase the awareness of the device cybersecurity capabilities for consumers to make informed purchases.

41. For professional-use-only devices, the affixing of the label is optional because measures are in place for professional bodies to purchase the appropriate devices.

42. Labelled devices will be listed in the CLS(MD) product list within the CSA website.

43. The proposed dimensions of the label are: 25 x 10mm (Small), 40 x 30mm (Medium) and 60 x 40mm (Large).

44. The larger-sized Cybersecurity Labels shall always be used. If the product packaging or the product has insufficient space, the smaller Cybersecurity Label shall be used. The Cybersecurity Labels shall not occupy more than 50% of the product packaging or the product where it is affixed to and shall be printed in an indelible manner with a minimum resolution of 300 pixels per inch.

45. Manufacturers are encouraged to use the Cybersecurity Labels in all advertisements and promotional materials of the labelled products in local print, broadcast, and digital media. This includes, but is not limited to, websites, online stores, and printed catalogues. However, the advertisements must

be of accurate contents and any inaccuracies in the labels used will be subject to the appropriate advertisement controls.

8.2 Validity of the Label

46. The Level 1 Cybersecurity Label is valid for a period of three (3) years, during which the developer is required to support the device with security updates. A self-declaration for CLS(MD) Level 1 requirements by the developer is required for renewal and to be submitted directly to CSA.

47. The Levels 2/3/4 Cybersecurity Labels are valid for the period in which the developer will support the device with security updates, up to a maximum of three (3) years.

48. The label could be revoked if any of the conditions in para 50 or 51 are met.

49. Before expiry of the label, a new CLS(MD) application is required to obtain a new label. This process can be initiated three (3) months before the expiry date of the existing label.

8.3 Labelling Principles

50. Upon receipt of the CLS(MD) label, the developer agrees to continuously adhere to the following principles:

a. The labelled product continues to fulfil the security requirements for the level that the product is being labelled with.
b. CSA shall be informed immediately of any changes that could affect the ability of the developer/product to fulfil the CLS(MD) requirements.
c. The developer must not make any statements about its product labelling that CSA deems to be misleading or unjustified. Examples include all models labelled when it is only a specific model that has been issued with the label; and claiming the product received a label of higher rating than what is being issued.
d. The developer must not use the Cybersecurity Label in any way that could discredit either MOH, CSA, HSA, IHiS), or CLS(MD).
e. The label must not be modified and shall be used exactly as issued by CSA.

8.4 Revocation of the Label

51. The developer is in breach of any terms of CLS(MD) requirements, and/or any other terms as agreed to in writing with CSA, if any of the following conditions is/are met:

a. The developer has failed to disclose any known or discovered vulnerabilities that, in CSA's opinion, can undermine the CLS(MD) label;
b. The developer fails to take any corrective measures during the grace period given by CSA, to the satisfaction of CSA;
c. The developer misuses the CLS(MD) label, CLS(MD) status, or any proprietary names and marks associated with CSA or CLS(MD);

d. The developer makes any statement that misrepresents any aspect of testing or the effect of the labelling under the CLS(MD);
e. CSA finds that the testing laboratory was in a position of conflict that impaired its ability to conduct a fair and impartial testing of the device;
f. The labelled device no longer meets the conditions under which the label was granted or does not meet any changed conditions for labels introduced by CSA after the device was originally labelled;
g. CSA discovered that the developer has made a false statement or declaration in any deliverables submitted to CSA.

9. Operationalisation

52. Application for the CLS(MD) labelling for Classes B, C and D devices shall be made via HSA's MEDICS platform, as per current practice for new medical device registration application, except for Special Access Route (SAR) devices.

53. Medical devices will have met Level 1 requirements prior to local market availability except for SAR devices. **Higher-level labelling will be voluntary, subject to developer's own business development model and individual healthcare institution purchasing requirement.**

54. SAR devices can also apply for CLS(MD) labelling. SAR devices (and all medical devices in general) that are not CLS(MD) labelled may not be allowed to be connected to public healthcare network after an appropriate stipulated sunrise period. This sunrise period will be determined and proposed separately, depending on the readiness of the developer and sector.

55. For Class A devices, existing HSA's process for self-declaration remains. No CLS(MD) label will be issued by default. Manufacturers who wish to obtain the CLS(MD) Level 1 label for labelling on the device shall additionally apply directly to CSA, submitting the declaration form, as well as corresponding evidences. The application will be reviewed in a similar manner to those of Class B to D devices, and approval given for them to include the label.

56. Due to the large volume and diversity of medical devices in the market, CSA would like to pace the implementation of the scheme by prioritising device types based on risk, impact to patient safety and risk, volume of use and connectedness. The proposed device categories are shown in Table 1 below and provided in the prescribed template for your feedback.

No.	Device categories
1	Radiological Imaging Devices (e.g. X-Ray, CT)
2	In-vitro Diagnostic Analysers (e.g. SARS-CoV-2 PCR machine)
3	Patient Monitors
4	Cardiac Electrical Implants (e.g. Pacemakers, cardiac monitor, implantable defibrillator)
5	Diabetic Management System (e.g. Continuous blood glucose sensor + Insulin pen + mobile app for insulin bolus calculation)
6	Insulin Pumps
7	Respiratory Ventilators

8	Clinical Decision Support Software (e.g. software to analyse CT chest images for detection of lesions)
9	Radiation Therapy System (For cancer treatment)
10	Medical Mobile Applications that run on general computing device (e.g. ECG app running on smartwatch)
11	Digital Therapeutic Software (e.g. deliver cognitive behavioural therapy for patients with substance Use Disorder)
12	Others

Table 1: Device categories

10. Devices that are currently in use

57. For classes A to D devices that were approved/declared prior to the implementation of the CLS(MD) and wish to obtain a CLS(MD) Level 1 label, manufacturers or vendors must perform a self-declaration for CLS(MD) Level 1 compliance with supporting evidence submission to CSA directly.

58. As existing devices have already been approved for use, they can remain in the market even if no labelling is sought. However, device use policies may impose limitations on purchase and use, in view of the cybersecurity threat landscape.

11. Feedback Sought

59. MOH, CSA, HSA, and IHiS welcome your comments and feedback on the framework, operationalisation, requirements for CLS(MD) testing laboratories, proposed design and conditions of the Cybersecurity Label, devices that are currently in use, and the application of the CLS(MD) framework.

60. This consultation will be held from 25 January 2023 to 3 March 2023.

61. Please email your feedback using the prescribed template to certification@csa.gov.sg by 3 March 2023. Using the prescribed template will ease our collation efforts. Where possible, you should highlight the specific area by the paragraph and/or line number in the proposed draft you are providing your comments.

62. Please provide your name, the organisation you represent, mailing address, contact number and email address within the prescribed template to enable us to follow up with you to clarify any issues, if necessary.

63. Your feedback is specifically sought for Sections: 6. Framework, para 21, 34 and 35; 7. Requirements for CLS(MD) Testing Laboratories; 8. CLS(MD) Labels; 9. Operationalisation, para 56; and 10. Devices that are currently in use.

64. Please note that the contents of any written feedback submitted, and the identity of the source, may be disclosed at the conclusion of this consultation. You may request for the feedback provided to be treated with confidence on grounds that the information is proprietary, confidential, or commercially sensitive. Such requests will be taken into consideration.

Annex A

CLS(MD) Certification Process

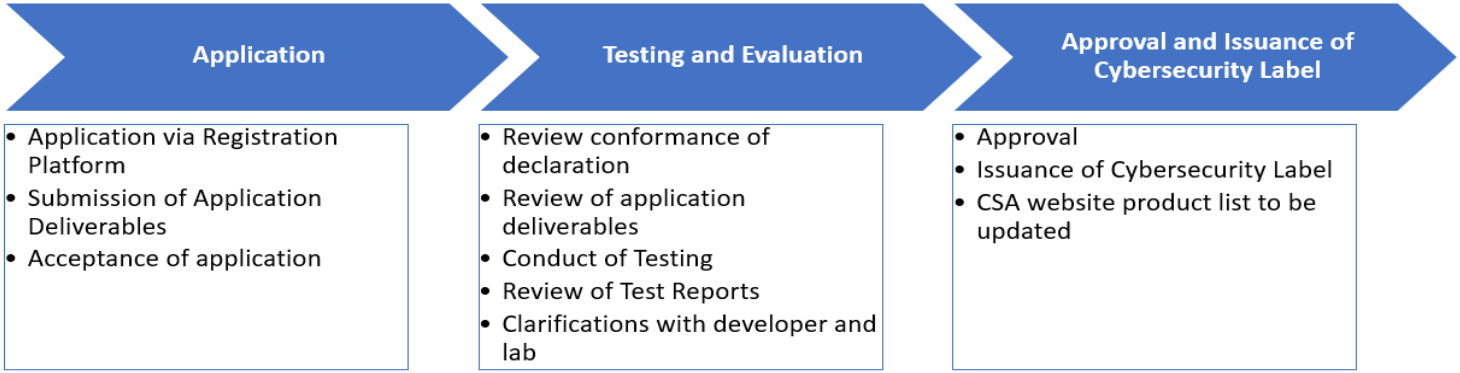

Figure 3 High level certification process

Evaluation and Testing	**Level 1**	**Level 2**	**Level 3**	**Level 4**
Declaration of Conformity to Security Baseline Requirements	Yes	Yes	Yes	Yes
Declaration of Conformity to Enhanced Security Requirements		Yes	Yes	Yes
Software Binary Analysis			Yes	Yes
Time-Bound Blackbox Penetration Testing			Yes	
Time-Bound Whitebox Security Evaluation				Yes

Table 2: Progressive Framework Assessment

In summary,

- CLS(MD) Level 1 applicants must meet the Security Baseline Requirements.
- CLS(MD) Level 2 applicants must meet the requirements from Level 1, and the Enhanced Security Requirements.
- CLS(MD) Level 3 applicants must meet the requirements from Level 2, conduct Software Binary Analysis and Time-Bound Blackbox Penetration Testing.
- CLS(MD) Level 4 applicants must meet the requirements from Level 3, and Time-Bound Whitebox Security Evaluation.

Annex B1

38 Clauses in the CLS(MD) Framework
Level 1
Note:
Mandatory and Conditional clauses are worded in this form, that a clause becomes mandatory when the conditions are met. For example, Mandatory (Conditional - Device makes use of an operating system) means that the clause provision is mandatory on the condition that the device makes use of an Operating System. Refer to Annex B3 for details on how to read the mandatory and conditional clauses.

Clause	Provision	Supporting Evidence Requirements	Clause Intent	Mandatory/ Conditional
Vulnerability Disclosure Policy				
1	The manufacturer shall provide a vulnerability disclosure program (i.e. ISO/IEC 29147, etc.) covering the device.	The vulnerability disclosure program (i.e. VDP website, etc.) shall be provided.	The objective of this clause is to ensure that the manufacturer has a **vulnerability disclosure program (VDP) covering the device**. The VDP should offer simple and clear information on how security researchers can **report product vulnerabilities to the manufacturer**. The VDP should include contact information (i.e. email address, phone number, web form, etc.) and may set communication expectations (i.e. the expected no. of days before the manufacturer provides an initial acknowledgement of receipt of the report, regularity of status updates for the reported vulnerability, etc.). The VDP is typically available on the manufacturer's webpage or alternatively, vulnerability disclosure platforms can also be used. Once a report has been received, it is expected that the manufacturer shall perform an investigation on the potential vulnerability. Once the manufacturer has confirmed that a vulnerability exists for the product, the manufacturer is required to disclose the vulnerability according to HSA's and CSA's requirements.	Mandatory

Cyber Security Product Upgrades (CSUP)				
7	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.	Software update plan outlining how software will be updated to maintain ongoing safety and performance of the device either regularly or in response to an identified vulnerability.	The objective of this clause is to ensure that the manufacturer have an **on-going postmarket plan to remediate cybersecurity vulnerabilities** to ensure device performance and safety is not compromised throughout the device's lifecycle.	Mandatory
10	The manufacturer shall have a Post-Market plan to proactively monitor and identify newly discovered cybersecurity vulnerabilities, assess their threat, and respond.	Supporting evidence shall describe the internal process for monitoring new vulnerabilities via reputable cybersecurity webpages (i.e. US CISA) or Information Sharing Organisation (i.e. ISAOs, ISACs etc.) and handling device vulnerabilities in a timely manner. For example, The evidence should include process diagrams, and shall describe the steps taken in the event a vulnerability is reported (i.e. receipt of vulnerability report, acknowledgement of receipt, investigation and review of the vulnerability, development and deployment of mitigating solution, communication with owners/operators, etc.).	The objective of this clause is to ensure that the manufacturer has in place a process to **monitor, identify and assess the device vulnerabilities, and to develop resolutions to address the identified vulnerabilities**. A well-defined vulnerability handling process will help to ensure that identified vulnerabilities are tracked and addressed, to minimize risk from vulnerabilities, to provide owner/operator with sufficient information to evaluate risks to their systems, and that security updates/patches or mitigation measures are available to address the vulnerability.	Mandatory

ROADMAP FOR MEDICAL DEVICE LIFE CYCLE (RDMP)				
20	The manufacturer shall consider cybersecurity risks/ vulnerabilities as part of their overall risk management process throughout the lifecycle of the medical device. It is highly recommended that manufacturer addresses cybersecurity risk related to universal default password and brute force attacks, where applicable. In addition, to provide evidence that the security of the device/effectiveness of the security controls have been verified.	Supporting evidence shall describe the following: a. Risk management plan that identifies, assess, implement mitigations to the relevant cybersecurity risks/ vulnerabilities to acceptable level and monitor the effectiveness of mitigation measures. b. List of cybersecurity controls measures in place (e.g. design controls) c. Security test reports and/or evidence to verify the security of the device and effectiveness of these security controls. The test document should contain the following information: -Descriptions of test methods, results, and conclusions; - A traceability matrix between security risks, security controls, and testing to verify those controls; and -References to any standards and internal SOPs/documentation used.	The objective of this clause is to ensure that the **manufacturer adopts a risk management process throughout the device lifecycle** to address any foreseeable cybersecurity risks. In addition, to demonstrate that the security of the device and effectiveness of security controls have been verified.	Mandatory

Level 2

Clause	Provision	Supporting Evidence Requirements	Clause Intent	Mandatory/ Conditional
Management of Sensitive Data				
2	The manufacturer shall have a list of sensitive data (such as personal identifiable information) that is collected and transmitted by the device.	Supporting evidence shall include the following: 1. List of all sensitive information and personal identifiable information that is collected by the device. 2. List of all sensitive information and personal identifiable information that is transmitted out of the device, and where these data are transmitted to (i.e., transferred to a database, remote storage location, removable media, back to manufacturer, etc.).	The objective of this clause is to ensure that the manufacturer is **aware of all sensitive data (such as personal identifiable information) that is collected, and where these information are transmitted to by the device**. This ensures that the manufacturer will not collect additional information that is not required. Examples of sensitive data not limited to the following: PII, User Password, User Credentials, cryptographic key data, etc.	Mandatory
Audit Controls				
3	The device logs or audit trails shall not store Personal Identifiable Information or sensitive data in clear text.	Supporting evidence shall describe how the device ensures that personal identifiable information or sensitive data are not displayed/printed in clear text in all logs or audit trails. In addition, sample logs and audit trails that show that personal identifiable information or sensitive data is not displayed or printed in clear text shall be provided.	The objective of this clause is to ensure that when devices **generate/create logs/reports for the purpose of facilitating investigations, audit and forensic analysis in the event of a cybersecurity incident**, such logs shall not display/print personal identifiable information or sensitive data in clear text. Methods such as masking of PII can be employed so that the logs or audit trails do not show this information. Examples of sensitive data not limited to the	Mandatory (Conditional - The device is not constrained)

			following: User Password, User Credentials, cryptographic key data, etc.	
4	The device shall be able to log actions and activities performed on the device.	Supporting evidence shall list and describe the types of actions and activities that are logged on the medical device. In addition, corresponding samples logs/audit trails containing the logged actions/activities shall be provided.	The objective of this clause 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**. Some examples of actions and activities that should be logged, not limited to the following: - Operating System Events (i.e. Start up and shut down of the system/services, network connection changes, changes or attempts to change security settings, etc.) - Application Account Information (i.e. Successful and unsuccessful log on attempts, log off attempts, application account changes, use of application privileges, etc.) - Application Operations (i.e. Application start up and shut down, failures, transactions, etc.)	Mandatory (Conditional - Device is not constrained)
Authorization (AUTH)				
5	The device shall ensure that only authorised users are permitted to access the functionalities/resources according to their assigned permission.	Supporting evidence shall describe the authorization mechanisms employed for preventing access to functionalities and resources from unauthorized users.	The objective of this clause is to ensure that the **device only permits authorised users to access the device and its functionalities/resources which they are authorised to**, applying the principle of least privilege.	Mandatory
6	The device shall be able to assign and segregate different roles (i.e. user,	Supporting evidence shall describe how the device supports the assignment and segregation of	The objective of this clause is to ensure that the **device supports the assignment and segregation of different roles and their**	Mandatory (Conditional -

	administrator and/or service accounts).	different roles, and shall list the following: - The different roles available on the device - The authorization/privileges for each role	**respective privileges**. This ensures that users are restricted to system functionality/resources/data that they are authorised to access.	Device is not constrained)
Cyber Security Product Upgrades (CSUP)				
8	The manufacturer shall have a process to notify and guide the owner/operator to achieve a successful software update through instruction manuals and procedures on installation when an update for any of the following components in the device has been tested and approved for installation. a. Operating System b. Driver and Firmware c. Anti-malware software d. Non-Operating System commercial off-the-shelf (COTS) components e. All other software (i.e., asset management software, license management software).	Supporting evidence shall describe the manufacturer's process for notifying owner/operator when updates for components in the device has been tested and approved for installation. Supporting evidence shall also include instructional manuals or guidance documents related to the installation of patches and/or software updates for the following shall be provided: - Device's Operating Systems - Device's Drivers and Firmware - Device's Anti-Malware software - Device's Non-Operating System commercial off-the-shelf (COTS) components - Other software components in the device (i.e., asset management software, license management software).	The objective of this clause is to ensure that the manufacturer **puts in place a process to notify and guide the owners/operators on the installation of patches and/or software updates** for the following components; a. Operating System b. Drive and Firmware c. Anti-Malware Software d. Non-Operating System commercial off-the-shelf (COTS) components. e. Other software components contained in the device (i.e., asset management software, license management software). in the device when updates for the device are available. This helps to ensure that owners/operators are alerted to the availability of any updates and can subsequently plan for the update of their devices at the earliest opportunity to reduce risk from vulnerabilities. The owner/operator should be **notified directly** (i.e., via email notifications, software alerts and notifications, etc.). Advisory postings on manufacturer's website (by itself and without notification) is insufficient as it is generally expected that owner/operator do not	Mandatory a. Mandatory (Conditional - Device makes use of an operating system) b. Mandatory (Conditional - Device makes use of Drivers and Firmware) c. Mandatory (Conditional - Device supports the use of anti-malware software) d. Mandatory (Conditional - Device makes use of COTS components) e. Mandatory

			have resources to actively monitor the manufacturer's website for available/new updates.	(Conditional - Device contains other software components such as asset management software, license management software, etc.)
Cyber Security Product Upgrades (CSUP)				
9	The device shall only allow installation of approved software.	Supporting evidence shall show and describe how the device/system only allows installation of approved software (i.e. digitally signed software, privilege controls for installation of software, etc.).	The objective of this clause is to ensure that the device has **mechanisms in place that prevents the installation of unapproved software**. Such installation of unapproved software results in the invalidated modification of the medical device or system and can adversely affect system performance or safety, and may open avenues for easy exploitation of identified vulnerabilities of the medical device. Some examples of how the device allows approved software installations, not limited to the following: - Digitally signed software by the manufacturer - Privilege controls for installation of software - No additional software can be installed beyond what the manufacturer has provided Some examples of how the device may prevent unapproved software installations, not limited to the following: - The device prevents the owner/operator from the installation of any software that is not approved or under explicit published guidance by the	Mandatory

			manufacturer. - The device has an authorization mechanism that prevents installation of the software that is not authorised by the owner/operator.	
Data Backup and Disaster Recovery (DTBK)				
11	In the event that the Medical Device handles non-transient data or data which is needed for further processing/storing, the device must provide the capability for the data to be backed up to remote storage or removable media.	Supporting evidence shall and describe how data (non-transient, or data which is needed for further processing/storing) can be backed up to remote storage or removable media.	The objective of this clause is to ensure that the device **provides the capability for backing up non-transient data, or data which is needed for further processing/storing** into either a remote storage or removable media.	Mandatory (Conditional - Device handles non-transient data or data which is needed for further processing/storing)
12	The device shall be able to back up system configuration information, patch restoration and software restoration.	Supporting evidence shall show and describe the following: - back up system configuration information - patch restoration and software restoration	The objective of this clause is to ensure that the **device supports the backing up of system configuration, patch restoration and software restoration**. In the event of a cybersecurity incident, the device can be restored to its intended working state and made operational.	Mandatory (Conditional - Device is not constrained)
Malware Detection/Protection (MLDP)				
13	The device shall have malware protection measures/mechanisms.	Supporting evidence shall describe how the device supports malware protection measures/mechanisms. If an anti-malware software is used, the name and version of the anti-malware software shall be provided. If other malware protection measures/mechanisms are used, a	The objective of this clause is to ensure that the **device have malware protection measures/mechanisms**. Some examples of malware protection measures/mechanisms, not limited to the following: - anti-malware software - secure boot - host-based intrusion detection/prevention - application whitelisting	Mandatory (Conditional - Device makes use of an operating system, Conditional - Device is not constrained)

		description of the mechanism and a rationale on how it meets the security objective of providing protection against malware shall be provided.		
Node Authentication (NAUT)				
14	The device shall support network access control mechanisms.	Supporting evidence shall describe the network access control mechanisms available on the device (i.e., internal firewall, network connection whitelist, communications only with authenticated devices).	The objective of this clause is to ensure that the **device allows access only to permitted entities/services/device**.	Mandatory (Conditional - Device communicates with other devices)
Connectivity Capabilities (CONN)				
15	The manufacturer shall provide the list of communication channels supported by the device.	Supporting evidence shall list of all communication channels available on the device.	The objective of this clause is to ensure that the **manufacturer provides a list of communication channels that are supported on the device**. Examples of communication channels, not limited to the following: - Wi-Fi - Bluetooth - ZigBee - LoRaWAN - NFC - Ethernet	Mandatory (Conditional - Device is able to communicate with other devices)
Person Authentication (PAUT)				
16	The device shall support and enforce authentication for all users and roles. Exception is when the emergency access (i.e. break glass) is activated. This would allow the device to continue to operate in	Supporting evidence shall describe the following: - all available device login-interfaces (i.e. device configuration portal, companion mobile application, user GUI, etc.) - authentication mechanisms (i.e.	The objective of this clause is to ensure that the device **enforces authentication for all users and roles**. For devices with one user/role, only a single set of authentication credential is required.	Mandatory

	Safe Mode or Limited Mode (with limited capabilities sufficient for use in emergency operations).	passwords, tokens, smart cards, digital signatures, biometrics, etc.) available for each of the device login-interfaces - all users and roles that are available on the device - accompanying screenshots showing the enforced authentication mechanisms	For devices with multiple roles (i.e. maintenance/service, administrator, user), different authentication credentials shall be used such that every user/role can be uniquely identified.	
17	The device shall support the changing of Authentication Method Reference Value (i.e. password, PIN, fingerprint, etc.) for all users and roles.	Supporting evidence shall show the mechanism(s) that can be used to change the authentication method reference value.	The objective of this clause is to ensure that the device **provides the capability for the authentication method reference value** (i.e. password, PIN, fingerprint, etc.) to be changed.	Mandatory
18	Where passwords are used and, in any state, other than the factory default, the medical device passwords shall be unique per device or defined by the user. Where pre-installed passwords are used, they shall be unique per device and sufficiently random.	Supporting evidence shall describe the following: 1. Does the device ship with factory default passwords that are universal across devices, with a pre-installed unique per device password, or does the device force the user to define a new password during initial setup? 2. If the device is shipped with a pre-installed unique per device password to avoid having universal default passwords, how are the pre-installed passwords generated for each device and what is done to ensure that the pre-installed passwords are sufficiently random? Are the randomised passwords based on any	The objective of this clause is to ensure that the **device does not utilise a universal default password**. Utilising universal default passwords has been the source of security problems. If one device is compromised, all devices with that factory universal default password can be compromised. If the device comes with a universal default password, the device shall force the user to define a new password during initial setup. The requirement can also be met **if the device is configured with pre-installed unique per device passwords**. These passwords must be unique per device and sufficiently random, and not related in an obvious manner to public information (i.e. MAC Address, Wi-Fi SSID, etc.).	Mandatory

		device information (MAC address, etc.)? The developer shall provide 5 instances of randomised passwords that are generated using the aforementioned password randomisation mechanism. Minimally, the following are required for pre-installed passwords: 1. Passwords with incremental counters ("password1", "password2") are not allowed. 2. Pre-installed passwords must be sufficiently randomised using a random function. 3. Passwords must not be relatable in an obvious manner to public information such as MAC address or Wi-Fi SSID. Please note that there are many mechanisms used for performing authentication, and passwords are not the only mechanism for authenticating a user to a device. If other authentication mechanisms are used, please provide details.		
19	The device shall have a mechanism available which makes brute force attacks on authentication mechanisms impractical.	Supporting evidence shall describe the employed authentication rate limiting policy for making brute force attacks impracticable on each of the device's login-interfaces.	The objective of this clause is to ensure that the **device is not susceptible to brute force attacks on authentication mechanisms.** **In emergency situations, if the authentication rate limiting mechanism is triggered, the**	Mandatory

		Examples of login-interfaces not limited to the following: • Device and/or device management portal login; • Companion Applications (i.e., Desktop/Mobile Application, etc.) • Other network interfaces, ports or services. For each of the login-interfaces available on the device, supporting evidence shall describe the following: 1. What is the maximum number of attempts within a certain time interval? 2. What happens when a certain number of failed authentication attempts is reached? Minimally, for each of the device's login-interfaces, the device shall employ a rate-limiting mechanism that has a limitation on the number of authentication attempts within a certain time interval, and locks/delays additional authentication attempts after a limited number of failed authentication attempts.	**emergency break-glass feature can be used**. Refer to Clause 16 - 'The device shall support and enforce authentication for all users and roles. Exception is when the emergency access (i.e. physical break glass) is activated)'. This would allow the device to continue to operate in Safe Mode or Limited Mode (with limited capabilities sufficient for use in emergency operations). Some examples (non-exhaustive) of authentication rate limiting mechanisms: • Throttling mechanism which introduces a random delay between authentication attempts • Account lockouts after a defined number of incorrect attempts • CAPTCHA • IP Address blocking after multiple failed logins • Two-factor authentication	

ROADMAP FOR MEDICAL DEVICE LIFE CYCLE (RDMP)				
21	The manufacturer shall follow a secure software development process during product development, such as ISO/IEC 27034 or IEC 62304, and shall evaluate third-party applications and software components included in the device as part of secure development practices.	Supporting evidence shall describe the following, and state the tools used for any of the secure software development process, adopted approaches, and other integrated security related activities conducted (if any). Examples: a. Descriptions of test methods, results, and conclusions; b. A traceability matrix between security risks, security controls, and testing to verify those controls; and c. References to any standards and internal SOPs/documentation used. d. How secure engineering approaches that have been adopted. Examples include the following: • Reuse existing, well-secured software: evidence showing the code repository used to store and maintain secured software for reuse when suitable, or internal documents describing the process for the storage and usage of secured software. • Secure coding practices: internal documents describing the process to ensure secure coding practices are followed during the development of the device. List the standard, guideline, security best practices that	The objective of this clause is to ensure that **the manufacturer adopts a secure product development lifecycle process and puts in place a process of evaluating third-party applications and software components before they are integrated into the device** during the development of the device. Typically, third-party applications and software components are used to reduce development effort, and it is crucial that the manufacturer evaluates these components carefully for vulnerabilities.	Mandatory

		are referenced. • Improve executable security: evidence showing compiler and build tools configuration, or internal documents describing the process to improve the executable security. • Functional testing of security features: test document such as functional testing test case document or test tool report describing the test cases (purpose and steps of each test case), or internal document(s) describing the process to conduct functional testing. • Developer and/or peer code review: Internal document or evidence of the tracking system used for tracking the code review feedback and remediation status of the findings. • Static application security testing (SAST): test report describing the result of SAST test or internal document(s) describing the process of SAST. • Dynamic analysis security testing (DAST): tool report describing the result of DAST test or internal document(s) describing the process of DAST. • Application programming interfaces (API) testing: tool report describes the result of API test or internal document(s) describing the		

		process of API testing. • Fuzz testing: tool report describing the result of fuzzing or internal document(s) describing the process of fuzz testing. • Penetration testing Supporting evidence shall describe the internal policy for evaluating third-party applications and software components as part of secure development practices. Some examples (not limited to the following) are: - Maintaining an inventory of components (including its version, applied patches and updates), and ensuring that all third-party applications and components are of the latest version with no known vulnerabilities. - Having a defined criteria for evaluation, selection, monitoring of performance and re-evaluation of such components/suppliers.		
22	The manufacturer shall maintain a web page (or through other avenues) to provide information on software support period and updates.	Supporting evidence shall include the URL of the manufacturer website that provides security information (i.e. Software support period, updates, security policies, security notifications, etc.).	The objective of this clause is to ensure that the manufacturer provides an **avenue for owner/operators to obtain information on software support period and updates**. Examples of how this could be achieved, not limited to the following: - Public website	Mandatory

			- Private website in which only owner/operators are granted access	
23	The manufacturer shall have a plan for managing third-party component end-of-life.	Supporting evidence shall describe the internal policy for managing third-party component end-of-life.	The objective of this clause is to ensure that the manufacturer has a **process to manage third-party component end-of-life.** The process helps to ensure that third-party components are monitored, and that actions/measures can then be planned and taken when these components reach the end-of-life.	Mandatory
SOFTWARE BILL OF MATERIALS (SBoM)				
24	The manufacturer shall provide the Software Bill of Material for the product's firmware and related mobile applications (iOS, Android), and other applicable software components (where applicable).	The Software Bill of Material for the firmware, related mobile applications (iOS, Android), and other applicable software components (where applicable) shall be provided.	The objective of this clause is to ensure that the manufacturer has a **software bill of material for the device, which would facilitate internal process of monitoring of the components used for the device and its associated vulnerabilities, and to deploy updates/remediation measures to maintain the device's safety and essential performance**. The software bill of material would also provide prospective owner/operator with visibility into the components used in the device and determine potential security risk.	Mandatory
SYSTEM AND APPLICATION HARDENING (SAHD)				
25	The manufacturer shall harden the device in accordance to industry standards.	Supporting evidence shall state the referenced industry standards and describe the measures taken to harden the device.	The objective of this clause is to ensure that the manufacturer **hardens the device in accordance to industry standards.** Some examples of industry standards, not limited to the following: - National Institute of Standards and Technology guidelines	Mandatory

			- OWASP Secure Medical Device Deployment Standard	
26	The device shall employ mechanism for software integrity checking.	Supporting evidence shall describe the mechanism used for ensuring software integrity (i.e., secure boot mechanism).	The objective of this clause is to ensure that the **device verify its software using secure boot mechanisms to make sure that the device boots using only software that is trusted by the manufacturer**.	Mandatory
27	All unnecessary resources and services (i.e., file shares, communication ports, protocols, and COTS applications etc.) which are not required for the intended use of the device shall be disabled/deleted.	Supporting evidence shall list all resources and services (e.g., file shares, communication ports, protocols, and COTS applications etc.) available on the device and their status (enabled/disabled), along with a description of the rationale behind enabling and disabling each of these resource/services.	The objective of this clause is to ensure that the manufacturer has **disabled all unused/unnecessary resources and services on the device to reduce attack surfaces.**	Mandatory
28	The manufacturer shall, by default, disable all communication ports and protocols (i.e., telnet, file transfer protocol [FTP], internet information server [IIS], etc.) that are not required for the intended use of the device. The manufacturer shall provide a list of network ports and protocols that are enabled/used on the device.	Supporting evidence shall list all communication ports and protocols available on the device and their status (enabled/disabled), along with a description of the rationale behind enabling and disabling each of these communication ports and protocols.	The objective of this clause is to ensure that the **device disabled all unused/unnecessary communication ports and protocols to reduce attack surfaces.**	Mandatory

SECURITY GUIDANCE (SGUD)				
29	The manufacturer shall provide security documentation for the owner/operator.	The security guidance documentation shall be provided.	The objective of this clause is to ensure that **security documentation is provided for the owner/operator**. The security documentation should aid and provide clear instructions for the owner/operator on how to configure and operate the device securely. The security guidance should also provide the owner/operator with guidance on how to check whether their device has been securely set up. The security documentation can be included within user guidance manuals or instructions for use.	Mandatory
30	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.	The guidance documents that show how the user may permanently delete data from the device or media shall be provided.	The objective of this clause is to ensure that the device **provides the capability for permanent deletion of data from the device or media in the event of decommissioning** of the device, or if the device is to be re-deployed.	Mandatory
31	The manufacturer shall provide documentation for factory created access accounts (including default accounts such as technician/service/administrator/etc.) in the devices.	The documentation for all factory created access accounts in the device shall be provided. In addition, a description of the rationale on the necessity for these default accounts shall be provided.	The objective of this clause is to ensure that the manufacturer is **aware of all default accounts available on the device, and that this information is documented and provided to the owner/operator to determine potential security risk from default accounts in the device**.	Mandatory
HEALTH DATA STORAGE CONFIDENTIALITY (STCF)				
32	The device shall support encryption of sensitive data at rest.	Supporting evidence shall address the following: 1. List all sensitive data and personally identifiable information that is collected or stored on the	The objective of this clause is to ensure that **all sensitive data is encrypted at rest.**	Mandatory (Conditional - Device is not constrained)

		device or removable media. 2. For encryption of data at rest, describe the cryptographic functions and algorithms used, corresponding cryptographic key sizes, and referenced standards (if any).		
TRANSMISSION CONFIDENTIALITY (TXCF)				
33	The device shall encrypt sensitive data prior to transmission via a network or removable media by default.	Supporting evidence shall address the following: 1. Describe how sensitive data is encrypted by default prior to transmission via network or removable media, and state the cryptographic functions and algorithms used, corresponding cryptographic key sizes, and referenced standards (if any). 2. List all data (i.e., operational logs, personally identifiable information, etc.) that would be sent back to the manufacturer.	The objective of this clause is to ensure that all **personally identifiable information is protected through the use of best practice cryptography <u>prior</u> to transmission via a network or removable media**. Some examples of how information can be encrypted prior to transmission via a network, not limited to the following: - Transport Layer Security (TLS) - Secure Bluetooth/ZigBee - DICOM - HL7 - IEEE 11073 - File encryption	Mandatory (Conditional - Device is able to communicate with other devices)
TRANSMISSION INTEGRITY (TXIG)				
34	The device shall support mechanisms (i.e. digital signatures, hash-based message authentication code) to ensure data is not modified during transmission.	Supporting evidence shall describe the mechanism(s) used to ensure data is not modified during transmission, and state the cryptographic functions and algorithms used, corresponding cryptographic key sizes, and referenced standards (if any).	The objective of this clause is to ensure that the **device uses best practice cryptography to ensure data integrity <u>during</u> transmission**. Some examples of how data integrity during transmission could be ensured, not limited to the following: - Transport Layer Security (TLS)	Mandatory (Conditional - Device is able to communicate with other devices)

		The corresponding network packet captures shall also be provided as supporting evidence.	- Hash-based message authentication code (HMAC)	
REMOTE SERVICE (RMOT)				
35	The device shall indicate when there is an enabled and active remote session.	Supporting evidence shall describe how the device indicates that there is an enabled and active remote session.	The objective of this clause is to ensure that the device provides an **indication to the owner/operator when there is an enabled and active remote session**. This aids the owner/operator in identifying possible unauthorised or suspicious remote session activities.	Mandatory (Conditional - Device supports remote sessions)
OTHER SECURITY CONSIDERATIONS (OTHR)				
36	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.	Supporting evidence shall describe how the remote administration functionality is implemented, how the remote administration functionality is secured, and include all necessary usage procedures.	The objective of this clause is to ensure that the **device implements remote administration securely and ensure that a remote user performing remote administration on the device can be clearly identified and deemed legitimate**. Technical means of meeting the objective would be the use of 2-Factor Authentication, Multi-Factor Authentication, dual-login (i.e. four-eyes principle approach which would require that the remote administration be initiated only after both the remote user and the local administrator have approved the request), or other feasible technical means. Alternatively, the manufacturer may also define procedural means (that the owner/operator should utilise if remote administration is to be used) which would achieve the same objective (i.e. Manual processes for verifying the identity of the remote user).	Mandatory (Conditional - if the device supports remote sessions)

37	The device shall employ recommended industry standard Wi-Fi security protocols (i.e. WPA2/3, etc.).	Supporting evidence shall show that WPA2 or higher shall be supported and used by default.	The objective of this clause is to ensure that the device **uses appropriate and recommended security protocol for Wi-Fi** (i.e. WPA2, or WPA3 if supported).	Mandatory (Conditional - if the device utilises Wi-Fi)
38	Local interfaces (i.e. USB, SD card readers) that support the use of removable storage media on the device or system shall be logically and/or physically disabled (i.e., tamper evident stickers, lindy port blockers) by default, if not required.	Supporting evidence shall list all local interfaces that support the use of removable storage. For each interface that is not required, describe the measure(s) taken to disable them logically/physically by default.	The objective of this clause is to ensure that **unused local interfaces shall be logically or physically disabled to reduce attack surface**.	Mandatory

CLS(MD) Conditions

Conditions	Description
Mandatory (Conditional - Device makes use of an operating system)	Examples of Operating Systems not limited to the following: - Microsoft Windows - Linux - Real-time operating systems (e.g. FreeRTOS, SafeRTOS, VxWorks, Nucleus, QNX, etc.).
Mandatory (Conditional - Device is not constrained)	RFC 7228: Small devices with limited CPU, memory, and power resources. Constrained node: A node where some of the characteristics that are otherwise pretty much taken for granted for Internet nodes at the time of writing are not attainable, often due to cost constraints and/or physical constraints on characteristics such as size, weight, and available power and energy. The tight limits on power, memory, and processing resources lead to hard upper bounds on state, code space, and processing cycles, making optimization of energy and network bandwidth usage a dominating consideration in all design requirements. Also, some layer-2 services such as full connectivity and broadcast/multicast may be lacking. Although constrained device are exempted to meet certain clauses, it is strongly recommended that constrained devices should still try to meet the requirement to ensure higher security.
Mandatory (Conditional - Device makes use of COTS components)	COTS refers to 'Commercial off the shelf'.