ANNEX A

The Ministry of Health (MOH), Cyber Security Agency of Singapore (CSA), Health Sciences Authority (HSA), and Synapxe (formerly known as IHIS) are collectively termed as the 'Workgroup' within the context of this document.

<u>Table A-1. Responses to key comments raised by respondents.</u>

1) Comments on Scope		**Workgroup's responses**
1.1	Multiple respondents sought clarification on the scope of medical devices, whether: a) medical devices that store personal identifiable information (PII) but do not have any communication capability are still in scope for CLS(MD). b) Software as a Medical Device (Sam) is in scope for CLS(MD).	For (a), the scope of the CLS(MD) applies to medical device as described in the First Schedule of the Health Product Act (Cap122D, 2008 Rev Ed) <u>and</u> have any of the following characteristics: i. Handle personal identifiable information (PII) and clinical data and has the ability to collect, store, process, or transfer such data; ii. Connect to other devices, systems, and services - Has the ability to communicate using wired and / or wireless communication protocols through a network of connections. More examples of in-scope and out-scope devices will be made available on the CSA website when the scheme is ready once the sandbox is launched. For (b), Software as a Medical Device (SaMD) will fall in scope if the device handles personal identifiable information (PII) and clinical data, or has the ability to collect, store, process, or transfer such data or connect to other devices, systems, and services.
2) Comments on Definition		**Workgroup's responses**
2.1	Regarding the use of terminologies within consultation, some respondents sought clarifications on:	For (a), the definition of terms will be made available on the CSA website when the scheme is ready at the sandboxing stage.

	a) definition of sensitive data, 'critical and significant vulnerabilities' b) standardisation of term ‘developer’ to ‘manufacturer’	For (b), the workgroup has taken these comments into consideration and will standardise the term ‘developer’ to ‘manufacturer’.
3) Comments on Background		**Workgroup’s responses**
3.1	Some respondents sought clarifications on whether the CLS(MD) is mandatory and if participation in CLS(MD) will impact the availability or speed of the device to market.	The CLS(MD) is a voluntary scheme and is independent from HSA's Medical Device Registration. Manufacturers may proceed to supply their medical devices in Singapore upon the completion of their registration with HSA and can choose to participate in the CLS(MD) on a voluntary basis. Nonetheless, manufacturers are strongly encouraged to participate in this scheme to ensure that the cybersecurity of your medical devices is being robustly tested and validated, which will give confidence in the branding of your medical devices marketed.
4) Comments on Framework Levels 1 & 2		**Workgroup’s responses**
4.1	Some respondents sought clarification on whether clauses #18 & #19 would be included into CLS(MD) Level 1 requirements.	The feasibility of including clauses 18 and 19 requirements as part of Level 1 is to uplift the baseline cybersecurity requirements which will be further explored under the CLS(MD) sandbox.
5) Comments on Framework Levels 3 & 4		**Workgroup’s responses**
5.1	One respondent suggested to include other forms of scanning capabilities performed using automated scanners (e.g., binary software composition analyser, malware scanner, and mobile application scanners).	For the CLS(MD), the intention is to leverage on the following tools for the analysis of the binary code: • Software Composition to detect Common Vulnerabilities and Exposures (CVEs) in third party components used. • Static Binary Code scanner to detect known software weaknesses (examples of known software

		weaknesses can be found in the Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Weaknesses list[1]). • Mobile Application Analysis. • Malware Scan. Details of this analysis will be confirmed and made available on the CSA website when the scheme is ready.
5.2	Some respondents queried on the template for declaration of conformity and supporting evidence.	For CLS(MD) Level 1 and Level 2, a template 'Declaration of Conformity' will be made available on the CSA website when the scheme is ready during the sandboxing stage. The requirements can be found in Annex B1 of the public consultation paper. Applicants are expected to indicate conformity (Yes/No/Not Applicable) to each of the clauses within the template, alongside descriptions of how the clauses are met, and indicate where the supporting evidence can be found (e.g., location of the chapter/section of the manufacturer's documentation).
5.3	One respondent proposed to premise the Minimum Test Specification (MTS) document on the ETSI EN 303 645 standard and sought clarification on the MTS requirements. Some respondents queried about the kinds of common attacks that are covered during the penetration testing.	The ETSI EN 303 645 and the corresponding ETSI TS 103 701 are intended for consumer IoT devices and would not be directly applicable to medical devices. The requirements for CLS(MD) are based on the Manufacturer Disclosure Statement for Medical Device Security (MDS2), which in turn can be mapped to IEC TR 80001-2-2:2012. The Minimum Test Specification (MTS) provides a minimum set of tests that must be performed by the test laboratory to ensure a common baseline testing across laboratories. The

[1] https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html

		set of tests included within the MTS are deemed as widely commonly known attacks, and hence their inclusion into the Minimum Test Specification (MTS). Minimally and not limited to the following, the MTS will cover at least the following areas: Ports and Services, Firmware, Firmware Updates, Communications, Configuration Portal, Mobile Application, and Authentication. The MTS will also cover other attacks that are particular to medical devices, and in the future, further tests may be specifically defined for certain device categories. A sample of a minimum test specification can be found in the CLS IoT - Minimum Test Specification[2]. The MTS for CLS(MD) will be made public as soon as it is available.
5.4	Regarding the documents required for testing, multiple respondents sought clarification on the following: a) What does 'guidance documents' and 'verification of guidance documents' refer to for penetration testing? b) What conformity verification of security requirements means for penetration testing? c) What does product security design documents refer to?	For (a), one of the sub-activities for penetration testing involves device setup and verification of guidance documents. The guidance documents refer to written material (service manual, operator manual etc.) that is intended to be used by the person maintaining and setting up the device (which could include end-users). The verification of the guidance documents refers to the act of the test laboratory investigating if the documentation would guide the user into i) setting up the device into a secure-by-default configuration and ii) setting up, maintaining, configuring, and using the device such that security can be ensured.

[2] https://www.csa.gov.sg/docs/default-source/our-programmes/certification-and-labelling-scheme/cls/publications/pub-cls-minimum-test-specification-v1-1.pdf?sfvrsn=c4f71dc3_0

		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. For (b), conformity verification refers to the test laboratory checking if the device has implemented the security requirements or measures that the manufacturer has declared in the submitted conformity checklist. This is to ensure that the manufacturer has not made false declarations/claims on the security functionality/measures of the device within the conformity checklist. For (c), Product security design documents refers a set of documents that aids the test laboratory in getting a better understanding of the security design of the medical device. This may include any of the following: • Security functionalities (e.g., Authentication and Authorisation, Cryptography, Secure Storage, Secure Communications, Audit) of the product and its functional specification • Security architecture (secure boot, self-protection, security domain separation, etc.) • Source code. These documents enable the test laboratory to perform Level 4 - Security Evaluation, which comprises more complex and targeted attacks which can only be achieved by having more thorough security design information.
5.5	Regarding resubmission of requirements when label is still valid (i.e., within 3-year validity period), multiple respondents requested to consider waiver of some requirements which have been already fulfilled by a lower-level label when applying for a higher level CLS(MD) label.	Applicants are required to submit a fresh application for the CLS(MD) level they are applying for and will have to resubmit all documentation required for the higher levels even if the existing label is still valid.

		The requirement for having to submit documentation is such that the applicant will have to ensure at the point of the application that the requirements for the current label continue to be met. This is an opportunity for the applicant to ensure that their submission is up to date, in the event of changes made to the medical device since the last application. It is anticipated that the review of requirements at the device's current level will take less time.
5.6	One respondent queried if testing could start before the CLS(MD) application. Some respondents sought more information on the following: a) Should the test report be made known to the manufacturers first? b) Whether software binary analysis is performed by the test laboratory, or by manufacturers and reviewed by test lab?	Applicants may choose to engage approved CLS(MD) test laboratories to perform testing prior to the formal application. However, there is a risk that the test may not be adequate or appropriate because the scheme body has not reviewed the test lab's proposed test plan approach and scope. CSA may request for more tests if necessary. For (a), the test report must be provided by the test laboratory to CSA directly. The test report shall contain the testing performed, test results, identified issues, and corresponding method of resolutions. CSA will liaise with the test laboratory on the test report. The test laboratory will work with the manufacturer on the issues. The manufacturer should expect to get a copy of the test report. For (b), the software binary analysis will be performed by the test laboratory, which will analyse the test results together with the manufacturer. More details on the application and labelling process will be made available on the CSA website when the scheme is ready during the sandboxing stage.
5.7	One respondent commented that penetration testing should be 'open box' and sought clarification on the reason why	The CLS(MD) is a voluntary scheme, and it is not mandatory for medical devices to meet Level 3 or Level 4 requirements.

	Level 3 and 4 tests are adopted when manufacturers have verified these medical devices for security requirements as part of ISO 13485. Some respondent requested to allow submissions of existing binary testing and penetration testing report or self-developed study reports, documenting compliance to CLS(MD), instead of having to go through third-party testing. Other respondents suggested to remove the black-box testing and keep white-box testing instead.	The use of approved 3rd party independent test laboratories ensures impartiality, consistency, and repeatability of the test results. These approved 3rd party test laboratories provide an independent assessment of the security of a medical device~~.~~ For Level 3 - Penetration Testing, the test laboratory would require minimally the guidance documents (setup guide, usage guide) as well as high-level information on the ports and services that are available on the device. With limited information on the design and the implementation of the security functionality, the test laboratory would only be able to conduct less targeted attacks, largely limited to the following areas: Ports and Services, Firmware, Firmware Updates, Communications, Configuration Portal, Mobile Application, Authentication. For Level 4 - Security Evaluation, the test laboratory would require more in-depth information such that they are able to conduct more thorough testing. For example, the test laboratory may require the security architecture, design details of implemented security functionalities, or source code. These details enable the test laboratory to analyse whether there are any inherent design weaknesses and to have a better understanding of how the security functionalities are implemented so that more targeted test cases can be devised and conducted. The benefit of Level 3 - Penetration Testing is that it allows the user/manufacturer to get a reasonable amount of assurance that the medical device is resistant to the common/basic attacks, without the need for high testing efforts and cost. Attacks such as brute forcing the authentication interface, privilege escalation attacks, command injections, cross-site scripting, firmware extraction

		and tampering, eavesdropping, utilising publicly available vulnerability scanning and exploitation tools, fuzzing, and more are commonly done at this level. At Level 4 - Security Evaluation, the end-user/manufacturer would be able to get higher assurance that the medical device would be resistant to more enhanced attacks since the medical device has been tested or reviewed at a more thorough level. At this level, the test laboratory would be provided more thorough security functionality implementation information for the device. With the additional information, the test laboratory will be able to identify weaknesses in the design and implementation of security functionalities and devise targeted enhanced attacks with the objective of breaking these security functionalities. For example, if the test laboratory would be provided information on how the device’s secure boot mechanism is implemented, the test laboratory may identify potential weaknesses and devise targeted attacks in overcoming the secure boot mechanism to boot a tampered firmware, thus gaining control over the device. Another example would be the extraction of encryption/secret keys from the device if the implementation for the secure storage of these cryptographic keys is weak. The difference between Penetration Testing and Security Evaluation is the approach taken by the test laboratory and the level of detailed device information made available to them.
5.8	There were comments on penetration testing duration which include: a) deciding the duration based on a risk-based criteria. b) deciding the duration based on device's complexity or device categories. c) allow manufacturers to decide testing duration.	The medical device manufacturer will be expected to provide a list of interfaces to aid the test laboratory in the conduct of their testing and evaluation. The proposed duration of 1 and 3 months for Level 3 penetration testing and Level 4 security evaluation serves as

	One respondent also proposed using a list of (physical/ logical) interfaces that manufacturers provide as base for a penetration test plan, and to include clear test framework to ensure comparable results and cost control.	a guidance on the duration the test laboratories should spend on penetration testing or security evaluation but could be adjusted to be longer or shorter depending on the actual scope necessary for the medical device. The period of 1 and 3 months is inclusive of the time spent by the test laboratory testing the device and excludes the other time required for administrative and logistical overheads. In addition, the test laboratory will need to perform minimal baseline tests that would be specified within the Minimum Test Specification. This will cover the commonly used ports/interfaces.
5.9	One respondent commented that device manufacturers should be given the rights to access the system impact and risk for the findings of the penetration test.	It is expected that the test laboratory shall work closely with the manufacturer during penetration testing and security evaluation on any discovered vulnerabilities/findings. The manufacturer and test laboratory may at any point in time, approach CSA to discuss and clarify these findings if necessary.
5.10	One respondent mentioned that test laboratories scans for vulnerabilities are not necessary as these vulnerabilities are constantly evolving and are moving targets. Some respondents commented that there should be a risk-based approach [i.e., based on intended use and the patient safety instead of solely on Common Vulnerabilities and Exposures (CVEs)] to analyse all identified issues from the test laboratories results.	Test laboratories scan for vulnerabilities are performed within software binary analysis by the test laboratory, which serves to provide an independent third-party analysis of the software binary test results. In addition, the results of the software binary analysis may be used by the test laboratory during penetration testing or security evaluation, to verify if the identified vulnerabilities are exploitable. For each vulnerability identified, the medical device manufacturer is expected to perform an assessment of the vulnerability and identify a method of resolution.

		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 test 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 test laboratory and the test laboratory will perform the first review of the suitability of this assessment. It is expected that at the end of this exercise, all identified vulnerabilities are accounted for, and no critical exploitable vulnerabilities should remain. All vulnerabilities and the corresponding method of resolution shall be provided to CSA for comments and review.
5.11	One respondent sought clarification if containerised applications (e.g., docker applications) are within scope of the software binary analysis.	These are applicable and within scope of the software binary analysis if they are part of the medical device.
5.12	Some respondents sought clarification on the following: a) minimum set of documents to provide to test labs. b) number of device units to provide to the test labs. c) how considerable-sized devices can be sent to the test labs for testing.	For (a), the documentation required depends on the intended CLS(MD) level. For Level 3 - Penetration Testing, the test laboratory would require minimally the guidance documents (setup guide,

		usage guide) as well as high-level information on the ports and services that are available on the device. For Level 4 - Security Evaluation, the test laboratory would require more in-depth information such that they are able to conduct more thorough testing. For example, the test laboratory may require the security architecture, design details of implemented security functionalities, or source code. These details enable the test laboratory to have a better understanding of how the security functionalities are implemented so that more targeted and better designed attacks can be conducted. For (b), the number of test units required for CLS(MD) Level 3 and Level 4 is dependent on the scope of the testing and the approach of the test laboratory. For instance, certain tests may potentially result in the failure of the device, in which the test laboratory may request for more samples of the device to ensure that testing may continue. Test laboratories may also request for more devices so that certain testing may be conducted in parallel to shorten testing efforts. For (c), manufacturers can choose to work with approved local and overseas test labs. For medical devices that have considerable size/weight, manufacturers may work with the test laboratory for testing to be performed on the manufacturer's premise. The list of approved test labs will be announced during the sandbox.
6)	**Comments on Requirements for CLS(MD) Testing Laboratories**	**Workgroup's responses**
6.1	Some respondents proposed to consider accepting test laboratories that do not meet ISO 17025 or are not members of IAF/ILAC but are able to comply with the test requirements of CLS(MD) Level 3 and Level 4.	We would like to invite respondents to kindly share the companies that can perform penetration testing but are not accredited to ISO 17025.

	Other respondents proposed to allow manufacturers to have internal testing laboratories to conduct tests instead of engaging an independent test laboratory due to cost.	ISO 17025 ensures that the test laboratory have in place appropriate management systems and procedures for ensuring that the quality of testing is performed in an adequate manner. In addition, these test laboratories should be able to demonstrate that it is impartial and that it and its personnel are free from any undue commercial, financial, and other pressures which might influence their technical judgement. On top of ISO 17025, CLS(MD) will require that these test laboratories demonstrate adequate technical competency to be able to carry out the level of testing as required under the scheme. All CLS(MD) test laboratories shall be independent laboratories, and should be free of any undue commercial, financial, and other interest of the medical device it would be testing.
6.2	Some respondents suggested to accept other security specific credentials such as ISO/IEC 27001, ISO 9712:2021 as not all overseas test laboratories have ISO/IEC 17025.	The scope of ISO 27001 differs from ISO 17025 and as such, ISO 27001 cannot be used as a specific credential or eligibility criteria for entry as an approved CLS(MD) test laboratory. Most testing inspection and certification test laboratories will have been accredited to ISO/IEC 17025. The respondent is invited to share the names of such entities so that CSA may further look into the topic and engage such entities. ISO 9712:2021 covers requirements for the qualification and certification of personnel who perform industrial non-destructive testing (NDT) in methods such as acoustic emission testing, eddy current testing, leak testing. It does not cover penetration testing.

		Therefore, the scheme will require that test laboratories are accredited to ISO 17025 which specifies requirements for competence, impartiality, and consistent operation of laboratories.
6.3	One respondent sought clarification on the minimum acceptable requirement of an appropriate security policy that does not comply to ISO/IEC 27001.	The purpose and intention of the security policy is to ensure that the staff members and the procedures undertaken by them maintain the high degree of security required to protect commercially sensitive information. The security policy should specify 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.
6.4	Some respondents requested for a list of approved test laboratories for both local and overseas.	A list of approved test laboratories for CLS(MD) will be published on the CSA CLS(MD) website. The list will comprise both local and overseas laboratories.
6.5	Some respondents sought clarification on the process of registering as a CLS(MD) approved test laboratory and whether any competency demonstration is required.	Test laboratories hoping to become an approved CLS(MD) test laboratory will have to apply to the CSA, after which CSA will assess if the laboratory has met the requirements of the scheme. Technical competency will be assessed through various channels such as technical exam, certification, as well as demonstration of technical skills through actual projects. More details will be made available on the CSA website when the scheme is ready during the sandboxing stage.
7) Comments on CLS(MD) Labels		**Workgroup's responses**
7.1	Some respondents queried on whether CLS(MD) labels should be affixed for non-professional use only (non-PUO) devices prior to importation or delivery. Another respondent	Affixing of the CLS(MD) label on non-PUO medical devices can be conducted prior or after importation into Singapore. Manufacturer's Licence is not required for the affixing of CLS(MD) labels on the device packaging, provided there is no

	queried whether HSA manufacturer's license is required for label affixing.	breach to the primary packaging that maintains the sterility or integrity of the medical device. However, the conduct of this activity should follow the Good Distribution Practice for Medical Devices (GDPMDS) principles.
7.2	Some respondents sought clarification on the level of packaging which label should be affixed on. Some respondents also queried on how label affixing can be done for products without physical form, and the requirements and label location for this scenario.	Physical labels should minimally be affixed on the primary packaging for non-PUO devices. Affixing to other parts of the non-PUO devices is optional. It is optional to affix labels on PUO devices. For products that do not have a physical form, labels can be deployed through electronic labelling, which will be shown within the graphical user interface of the medical device. Electronic labelling shall only be used for SAMD or devices that do not have a physical form.
7.3	One respondent sought clarification on whether the CLS(MD) label is for the device or specific hardware and software version of the device. Some respondents also queried if manufacturers are required to apply for new label when software updates are installed for devices.	The CLS(MD) label is issued to the medical device. The label will remain valid for up to 3 years from date of label issuance, as long as the device continue to fulfil the CLS(MD) requirements and that software updates/changes to the medical device are minor (i.e., changes in graphical user interface, changes that do not affect the security functionality, etc.). However, if the hardware or software changes are deemed major (i.e., changes to the operating system, changes to the programming language used, major changes to the security functionalities, etc.) as per CLS(MD) requirements, the manufacturer may be required to engage a test laboratory to undergo assurance testing to maintain the validity of the label. This is part of ensuring that the device remains secure despite the major changes.

7.4	Some respondents proposed further features to the label, which include: a) adding URL link in the label, which directs to label directory housing device information and registration ID. b) removal of validity date on label. One respondent also sought clarification on whether the application ID is the same as the label ID. Some respondents also queried if it is possible to print labels in black and white.	For (a), the CLS(MD) label will contain a QR code which directs the user to the exact product listing within the CLS(MD) product list within the CSA website. For (b), the validity date will not be printed on the label. Users of the label may scan the QR code to view the validity date on the CSA website. The application ID is different from the label ID. The label ID is only issued upon the completion and approval of the application. The CLS(MD) label shall be printed in its original colour.
7.5	Some respondents proposed flexible label validity for different devices based on their support lifecycle, rather than a fixed time-period of 3 years. Some also suggested having auto-renewal option instead as resubmission and testing every 3 years may increase administrative burden and not be feasible for Singapore's small market.	As the threat landscape is continuously evolving, there is a need to ensure that devices are still compliant with the CLS(MD) requirements. As such, application for renewal is required. The label validity of up to 3 years ensures a balance between operational needs and cybersecurity assurance. More details will be made available on the CSA website when the scheme is ready.
7.6	Some respondents sought clarification on renewal requirements for CLS(MD) Levels 2-4 and proposed redefining renewal period based on CLS(MD) levels. Other respondents queried if the current registration ID will remain the same after the renewal and if there is a need to replace old labels upon renewal.	More details on renewal requirements for CLS(MD) Levels 2 - 4 will be provided on the CSA website when scheme is ready. The medical device may retain the existing label ID upon renewal.
7.7	Some respondents sought clarification on whether new labels will be issued with change notification. Other respondents proposed having a list of changes that requires	New CLS(MD) labels will not be issued with change submission as the CLS(MD) label itself does not include the validity date. Details on the list of changes and process of

	reporting to CSA and some guidance on the process of change notification.	change notification will be provided on the CSA website when the scheme is ready.
7.8	Some respondents sought clarifications on how vulnerabilities should be reported.	Reporting to CSA may be done through email cls_md@csa.gov.sg or through other mechanisms to be introduced in the future. If vulnerabilities impact patient safety and device performance, HSA's GN-05 Guidance on the Reporting of Adverse Events and GN-10 Guidance on Medical Device Field Safety Corrective Action should be referenced.
7.9	Some respondents sought clarification on how to manage physical labels affixed on devices in the event the label has been revoked or expired. One respondent also queried on the communication and remediation process if breach is discovered.	Upon the revocation or expiry of a label, the manufacturer and the test laboratory shall immediately cease all use of the CLS(MD) label and desist from holding the applicable products out as being labelled under the CLS(MD). On the CSA website, the device will then be removed from the CLS(MD) labelled product list and subsequently listed in the historical product list. Manufacturers should report the vulnerabilities/breaches to CSA via cls_md@csa.gov.sg or other mechanisms to be introduced in the future. CSA reserves the right to revoke the CLS(MD) label should it be discovered that the device has met the following conditions: • falsely declared to have met the CLS(MD) requirements but have not done so. • failed to disclose any known or discovered vulnerabilities that, in CSA's opinion, can undermine the CLS(MD) label. • in breach of any terms and conditions of the CLS(MD).

8)	Comments on Operationalisation	Workgroup's responses
8.1	Multiple respondents requested further information on the paced implementation of devices, with respect to: a) further segregating implementation based on risk class. b) change in implementation timeline. c) clear prioritisation criteria. d) examples of 'Other' category of devices.	The next phase of CLS(MD) implementation will be the sandbox approach. The sandbox approach will allow stakeholders (applicants, scheme body, testers) to work through the finer technical and operational aspects and details of the scheme on a smaller scale first before mainstreaming it.
8.2	One respondent sought clarification on what connection to the public healthcare network entails, whether any network connection, be it Bluetooth or local network also falls within the scope.	Any means of communication with the hospital network, be it through wired and / or wireless communication protocols using a network of connections can be considered as connected to the healthcare network.
8.3	Regarding Special Access Routes (SAR) devices, some respondents sought clarification on: a) whether CLS(MD) requirements applies to SAR devices. b) requirements needed for SAR devices to connect to the healthcare network and that CLS(MD) levels should be aligned with purchasing requirements from Public Healthcare Institution. c) sunrise period for mandating SAR devices to be labelled to connect to the public healthcare network.	For (a), CLS(MD) is a voluntary scheme, and all new and existing devices can apply for the label. For (b), SAR devices will be subjected to cybersecurity requirements if they are connected to the healthcare network and as such, we encourage manufacturers to apply for CLS(MD). CLS(MD) could be incorporated by healthcare institutions in the future as part of purchasing requirements. For (c), sunrise period for mandating SAR devices to be labelled to connect to the public healthcare network will be determined when the proposed Health Information Bill is promulgated and enforced in 2025.
8.4	Some respondents proposed leveraging existing practices and approvals to review cybersecurity in medical devices instead of adopting this labelling scheme. The rationale was that medical devices would have met cybersecurity requirements prior to marketing in US and EU and as such this scheme would not have significant additional value.	The requirements of CLS(MD) consists of a framework of 4 cybersecurity levels (from meeting basic and enhanced cybersecurity requirements, to undergoing penetration and security evaluation) to rate medical devices according to their levels of cybersecurity provisions. Through the CLS(MD) label, we hope to enable healthcare institutions and consumers to make more informed purchasing decisions.

8.5	Some respondents sought clarifications on whether: a) Professional Use Only (PUO) Class A devices will be issued with CLS(MD) label by default if they are declared on HSA Medics and meets all level 1 clauses and queried if the same is applied to Class B, C, D devices. b) it is mandatory for non-PUO Class A devices to be affixed with CLS(MD) label and whether there is a need to apply with CSA if affixing of CLS(MD) label is not necessary for PUO devices.	Devices must apply to CLS(MD) separately and meet the CLS(MD) requirements corresponding to the level applied for to get a label, regardless of Class A, B, C or D. All new and existing devices can apply for the label. For (a), CLS(MD) level 1 label will not be issued to Class A MDs by default. The label will only be issued after CSA has reviewed all level 1 requirements. In addition, the feasibility of including clauses 18 and 19 requirements in CLS(MD) level 1 will be explored under the CLS(MD) sandbox. The finalised CLS(MD) level 1 requirements will be released after the conclusion of the CLS(MD) sandbox. For (b), it is mandatory for non-PUO Class A devices to be affixed with CLS(MD) label if manufacturers wish to apply these devices to the voluntary CLS(MD) and are awarded with the label.
8.6	One respondent queried if HSA registration of a medical device and the review of the declaration of conformity are separated processes and if separated packages of documentation will need to be provided when applying for CLS(MD).	HSA registration of a medical device and the review of the declaration of conformity in CLS(MD) are separate processes. Manufacturers interested to apply for CLS(MD) will need to send in a separate application and upload the packages separately via GoBusiness Licensing Portal. The same process applies to all classes of devices. More details on this application process will be made available on the CSA website when the scheme is ready.
8.7	Some respondents queried on specific details of the CLS(MD) process: a) Key roles and responsibilities of manufacturers, CSA, and HSA. b) Turn-around time for review of CLS(MD) application for new devices and for label renewal.	More details on this aspect will be made available on the CSA website when the scheme is ready. Note that for the stipulated duration for time-bound penetration testing excludes time taken for

	c) Application process for change notification. d) Application process and application platform for SAR devices. e) Application fees of CLS(MD).	administrative/logistical overheads (surface test plan, rectification of vulnerabilities).
9)	**Comments on Devices Currently in Use**	**Workgroup's responses**
9.1	A few respondents commented on the possible adverse impacts of implementing CLS(MD) on devices currently in use, potentially leading to huge costs for extensive product redesign or reduced availability of product in the market if they do not meet the minimum requirements of Level 1. Few respondents also queried on how future changes (e.g., software updates, change notification) will affect devices currently in use and if any actions need to be taken with relation to the scheme.	The CLS(MD) is voluntary and will have provisions in place for devices that are already approved for use before the launch of the scheme. This is to ensure patient care can continue. Therefore, implementation of the scheme should not restrict market availability or force the manufacturers to undertake huge costs to extensively redesign their existing products. All devices currently in use should be assessed for Level 1 requirements minimally. Should they not be able to comply, healthcare entities may choose to conduct a risk assessment based on the intended use and remediate any identified risk accordingly to ensure devices can fulfil the use case requirements. If the residual risk is acceptable, the devices can continue to be used. Guidance will also be provided to healthcare entities to include cybersecurity requirements when they intend to procure new devices. Should the device currently in use be CLS(MD) labelled when a software update is available or change notification is approved, the manufacturer should 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 manufacturer/product owner to fulfil the CLS(MD) requirements.

		c) The manufacturer 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 manufacturer must not use the Cybersecurity Label in any way that could discredit either MOH, CSA, HSA, Synapxe), or CLS(MD). e) The Cybersecurity Label must not be modified and shall be used exactly as issued by CSA. Regardless of whether the device is labelled under the CLS(MD), the manufacturer should ensure that the customers are made known of the changes, especially if it is security related, to conduct a risk assessment where necessary and install the updates.
9.2	Multiple respondents requested further information of the device use policies that may impose limitations on purchase and use: a) Will there be timeline of allowing devices with no CLS(MD) labelling to remain in the market? b) Clarity on types of limitations.	The CLS(MD) is voluntary and will have provisions in place for devices that are already approved for use before the launch of the scheme. This is to ensure patient care can continue. Thus, implementation of the scheme should not restrict market availability or force the manufacturers to undertake huge costs to extensively redesign their existing products. For (b), device use policies may be entity-specific commensurate with its risk appetite. Prescribing device use policy is outside the scope of the scheme. However, guidance will be provided to healthcare entities to include cybersecurity requirements when they intend to procure new devices.

10)	Comments on General Topics	Workgroup's responses
10.1	One respondent queried if there would be a 'simplified' procedure to apply for CLS(MD) if the product has already achieved a label similar to CLS(MD) overseas.	There is currently no similar scheme overseas. However, attaining international mutual recognition remains a key motivation of CLS(MD) and we will review the topic again once partner(s) have been identified.
10.2	One respondent commented that there should be more clarity on the mechanisms for CSA to randomly check compliance.	For all CLS(MD) applications, all supporting evidence (e.g., documentation, technical testing) will be thoroughly vetted by CSA to meet the compliance requirements before the label can be issued. Once the label is issued, it is the responsibility of the manufacturer to ensure that the product continues to fulfil the security requirements for the level that the product is labelled with. This reflects the manufacturer's commitment to provide updates for vulnerabilities and security features. As such, the label will only be valid for devices that have not reach cybersecurity end-of-support (EOS). Also, should any future changes affect the product/manufacturer's ability to meet the scheme's labelling principles, it will be subjected to label revocation.
10.3	One respondent commented that the scheme has limited reference to international standards and may not be sufficient for global medical device manufacturers to adopt in their manufacturing processes. As such, this may lead to restricted market availability or high cost to redesign the product.	The requirements in CLS(MD) Levels 1 & 2 are compiled and titrated from existing guidelines, standards, and requirements already in use in Singapore (public healthcare policies, national standards like TR67, existing CSA Cybersecurity Labelling Scheme for IoT framework, and incorporate international guidelines and recommendations published by IMDRF, NEMA-MDS2, NIST). Furthermore, the CLS(MD) is voluntary and will have provisions in place for devices that are already approved for use before the launch of the scheme. This is to ensure patient care can continue. Thus, implementation of the scheme should not restrict market availability or force the

		manufacturers to undertake huge costs to extensively redesign their existing products. That said, it is strongly encouraged for all devices currently in use to be assessed for Level 1 requirements minimally. Should they not be able to comply, healthcare entities may choose to conduct a risk assessment based on the intended use and remediate any identified risk accordingly to ensure devices can fulfil the use case requirements. If the residual risk is acceptable, the devices can continue to be used. Guidance will also be provided to healthcare entities to include cybersecurity requirements when they intend to procure new devices.
10.4	One respondent proposed to map the CLS(MD) levels to the security level of the use environment required for the medical device.	While assessing cybersecurity posture from a use case/operating environment perspective is valid, the use cases may change rapidly due to the complex evolving and dynamic healthcare environment; and thus, not operationally feasible.