HEALTH SCIENCES AUTHORITY

August 2026

Best Practices Guide for Medical Device Cybersecurity

Revision 1

HSA Health Sciences Authority

CONTENTS

REVISION HISTORY

Guidelines Version (Effective Date) *[3 latest revisions]*	Revision
GL-10 Best Practices Guide for MD Cybersecurity: *First Release* (17 August 2026)	R1

Changes and updates made in each document revision are annotated with or within the arrow symbol "►". Deletions may not be shown.

1. INTRODUCTION

As healthcare technology advances, medical devices are becoming increasingly connected and reliant on software. These changes bring significant benefits to patient care, but they also introduce new risks. If these risks are not properly managed, they could result in patient harm or delays in treatment.

This document is intended to help medical device manufacturers, product registrants, importers, local authorised representatives, and healthcare providers understand how to maintain security of connected medical devices placed on the Singapore market. It shares practical advice on cybersecurity across the device's entire life cycle, from development (pre-market stage) through to use and maintenance (post-market stage). The responsibilities of healthcare providers described in this guide commence from the **Support stage**, when devices are supplied, installed, or already in use in Singapore.

The pre-market stage is when the medical device is being developed. At this point, it's important to incorporate cybersecurity into the device from the outset. This includes designing strong security features (known as Secure by Design), planning how to manage risks, testing the device for security issues, preparing clear user instructions and documents, and creating a plan for keeping the device secure after it's released. It also involves listing all the software components used in the device, which is called a Software Bill of Materials (SBOM).

The post-market stage covers the period after a connected medical device is placed on the Singapore market, including devices that are already installed and in use. Cybersecurity risks may emerge during this period and should be managed appropriately. This stage is divided into three parts. In the **Support stage**, the device receives regular updates and maintenance to protect it from new threats. In the **Limited Support stage**, the device continues to receive some security support, but at a reduced level. In the **End of Support stage**, the device is no longer actively supported, and additional measures may be needed to manage the risks of continued use.

By following these best practices throughout the Total Product Life Cycle (TPLC) of connected medical devices placed on the Singapore market, manufacturers, product registrants, importers, local authorised representatives, and healthcare providers can help keep devices secure, protect patients, and support the safety of healthcare systems. As the cybersecurity landscape and technologies such as artificial intelligence continue to evolve, stakeholders should remain informed and adapt their cybersecurity strategies accordingly.

2. SCOPE

This document does not constitute regulatory guidance and does not establish regulatory requirements or expectations for pre-market submission or registration. Instead, it provides practical recommendations for managing cybersecurity throughout the TPLC of all connected medical devices placed on the Singapore market, including connected general medical devices and In-Vitro Diagnostic (IVD) devices, whether for professional use only (PUO) or non-PUO. It applies to devices newly supplied in Singapore as well as devices already installed and in use.

The purpose of this document is to help manufacturers, product registrants, importers, local authorised representatives, and healthcare providers understand and apply fundamental cybersecurity principles. The recommendations encompass the entire TPLC of connected medical devices placed on the Singapore market. Manufacturer-related recommendations commence at the Development stage, while the responsibilities of Singapore healthcare providers described in this guide begin at the **Support stage** and continue through the **Limited Support** and **End of Support stages**.

3. DEFINITIONS

Asset: physical or digital entity that has value to an individual, an organisation or a government. (IMDRF/CYBER WG/N70)

Attack: attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset. (IMDRF/CYBER WG/N60)

Availability: property of being accessible and usable on demand by an authorised entity. (IMDRF/CYBER WG/N70)

Confidentiality: property that information is not made available or disclosed to unauthorised individuals, entities, or processes. (IMDRF/CYBER WG/N70)

Cybersecurity: a state where information and systems are protected from unauthorised activities, such as access, use, disclosure, disruption, modification, or destruction to a degree that the related risks to confidentiality, integrity, and availability are maintained at an acceptable level throughout the life cycle. (IMDRF/CYBER WG/N70)

Common Vulnerability Scoring System (CVSS): CVSS provides a numerical score based on several metrics, including exploitability, impact, and complexity, to assess the severity of a vulnerability. The base score reflects the intrinsic qualities of a vulnerability and ranges from 0.0 to 10.0, with 10.0 being the most severe. CVSS also includes temporal and environmental scores to account for factors such as the availability of patches and the specific environment in which the vulnerability exists. (https://www.first.org/cvss/)

End of Life (EOL): Life cycle stage of a product starting when the manufacturer no longer sells the product beyond their useful life as defined by the manufacturer and the product has gone through a formal EOL process including notification to users. (IMDRF/CYBER WG/N60)

End of Support (EOS): Life cycle stage of a product starting when the manufacturer terminates all service support activities and service support does not extend beyond this point. (IMDRF/CYBER WG/N60)

Exploit: defined way to breach the security of information systems through vulnerability. (IMDRF/CYBER WG/N70)

Integrity: property whereby data has not been altered in an unauthorised manner since it was created, transmitted or stored. (IMDRF/CYBER WG/N70)

Patient Harm: physical injury or damage to the health of patients. (IMDRF/CYBER WG/N60)

Professional Use Only (PUO) medical device: a medical device that is to be used on an individual solely by, or under the supervision of, a qualified practitioner. (HEALTH PRODUCTS ACT 2007/HEALTH PRODUCTS (MEDICAL DEVICES) REGULATIONS 2010)

Qualified practitioner: a registered medical practitioner under the Medical Registration Act 1997, when acting in the course of providing medical treatment to a patient under his care; or a registered dentist under the Dental Registration Act 1999 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. (HEALTH PRODUCTS ACT 2007/HEALTH PRODUCTS (MEDICAL DEVICES) REGULATIONS 2010)

Security testing: type of testing conducted to evaluate the degree to which a test item, and associated data and information, are protected so that unauthorised persons or systems cannot use, read, or modify them, and authorised persons or systems are not denied access to them. (IMDRF/CYBER WG/N70)

Software Bill of Materials (SBOM): list of one or more identified components, their relationships, and other associated information. (IMDRF/CYBER WG/N70)

Threat: potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. (IMDRF/CYBER WG/N70)

Total Product Life Cycle (TPLC): Development, Support, Limited Support, and End of Support Stages in the life of a medical device. (IMDRF/CYBER WG/N70)

Vulnerability: weakness of an asset or control that can be exploited by one or more threats. (IMDRF/CYBER WG/N70)

4. GENERAL PRINCIPLES

Effectively managing cybersecurity risks across the entire life cycle of a connected medical device placed on the Singapore market is essential to protect patient safety and ensure device performance. All relevant stakeholders, including manufacturers, product registrants, importers, local authorised representatives, and healthcare providers, should understand their respective roles and work together.

Cybersecurity should not be treated as a separate set of discrete tasks, but as an interconnected series of actions that mutually reinforce one another. This approach moves away from reactive problem-solving and instead focuses on embedding security into every stage of the device's life cycle. It recognises cybersecurity as an on-going effort that demands continuous attention, updates and improvements to keep pace with emerging threats.

The next sections of this guide explain the key principles that support strong cybersecurity for medical devices. These include **Shared Responsibilities**, which highlight the need for teamwork among all parties involved; **Transparency and Communication**, which encourage the sharing of information; and **Secure by Design**, which means building security into the device from the outset.

4.1 Shared Responsibilities

Keeping connected medical devices secure is a shared responsibility across the supply and use chain. Manufacturers, product registrants, importers, local authorised representatives, and healthcare providers should understand their respective roles and work closely together to monitor, assess, reduce, and respond to cybersecurity risks throughout the device's life. Manufacturers remain responsible for incorporating appropriate cybersecurity measures into device design and life cycle planning, while healthcare providers assume operational responsibilities from the **Support stage**, when devices are supplied, installed, or in use in Singapore.

Manufacturers should regularly update and improve their medical devices to address evolving cybersecurity threats. Product registrants, importers, and local authorised representatives should support timely communication and implementation of relevant

cybersecurity measures in Singapore. Healthcare providers should not be expected to carry the full responsibility for device cybersecurity while manufacturer support remains available.

While technical experts play an important role in keeping medical devices secure, it is senior management within both manufacturing organisations and healthcare providers who make key decisions about changes and improvements. Their active support and leadership are essential to ensure that cybersecurity is properly managed throughout the device's life cycle.

4.2 Transparency and Communication

Sharing cybersecurity information is a key part of keeping medical devices safe throughout their life cycle. Manufacturers, product registrants, importers, local authorised representatives, and healthcare providers are encouraged to share relevant updates, report issues, and work together to manage risks. This includes coordinated vulnerability disclosure and timely communication to affected users in Singapore.

When both parties remain engaged, they can better plan and respond at each stage of the device's life cycle. For example, manufacturers should inform users in advance when software support is ending, so healthcare providers can take the necessary steps. Clearly defined and accessible communication channels should be established to ensure that pertinent information is effectively disseminated to relevant stakeholders in a timely manner.

4.3 Secure by Design

Secure by Design means building cybersecurity into a medical device right from the outset. This approach looks at possible risks and weaknesses during every step of development, from early planning to deployment and on-going maintenance.

By incorporating security features in the device's core design, the result is a stronger and more reliable product that is better able to resist cyberattacks. This not only improves the device's safety throughout its life cycle but also reduces the need for expensive fixes and updates subsequently.

5. OVERVIEW OF TPLC

Cybersecurity risks should be considered at every stage of a medical device's life cycle. The TPLC approach helps relevant stakeholders remain prepared for and respond to the evolving cybersecurity landscape. For connected medical devices placed on the Singapore market, the TPLC encompasses device design, stakeholder responsibilities, and risk management from development through End of Support. Healthcare provider responsibilities under this guide commence from the **Support stage**.

The TPLC of a medical device includes several stages: **Development**, **Support**, **Limited Support** and **End of Support**. It is important to manage cybersecurity risks at every stage.

The later stages, End of Life (EOL) and End of Support (EOS), are especially critical. EOL means that the manufacturer no longer sells the product beyond its defined useful life and support may be reduced. EOS means that the manufacturer has terminated service support activities. For devices that were previously placed on the Singapore market with an adequate manufacturer-supported cybersecurity life cycle, operational responsibility for managing the risks of continued use after EOS shifts to the healthcare provider. This transfer does not remove any continuing responsibilities that may apply to manufacturer, product registrant, importer, or local authorised representative, including communication of known safety risks and applicable regulatory reporting obligations.

Therefore, close collaboration between manufacturers and healthcare providers is essential to ensure that devices remain reasonably protected against cybersecurity threats throughout their life cycle.

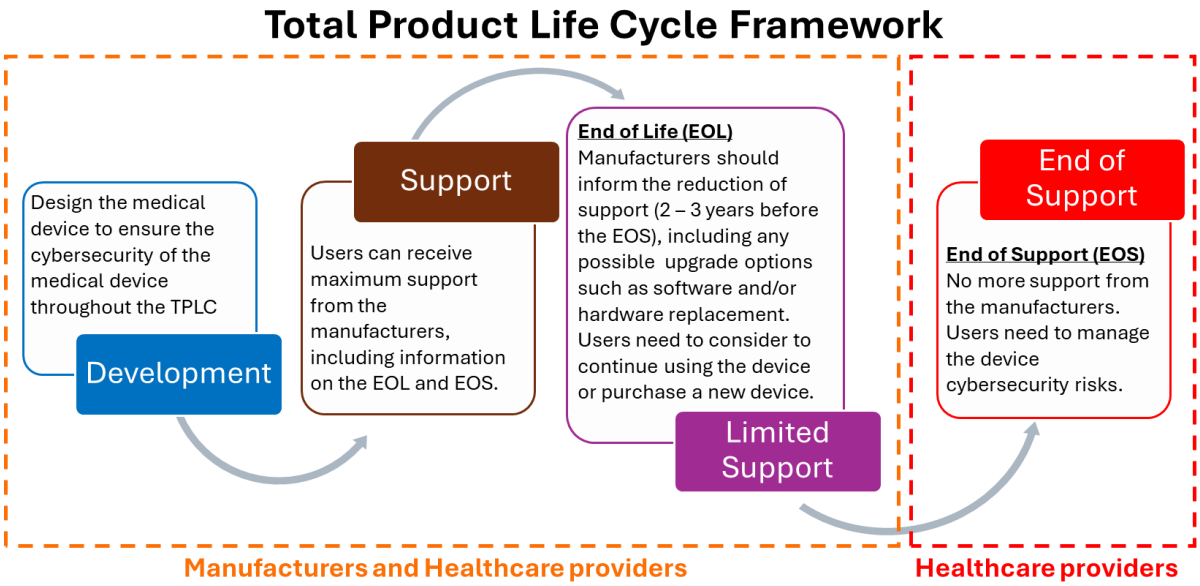

Figure 1: Total Product Life Cycle Framework

6. PRE-MARKET – DEVELOPMENT STAGE

Medical device manufacturers should make cybersecurity a priority throughout the entire product life cycle. During the development stage, there are specific areas to focus on to help keep the device secure over time. These include designing strong security features, planning how to manage risks, testing the device for security issues, preparing clear user information, and creating a plan for keeping the device secure after it's on the market.

Manufacturers should also prepare a Software Bill of Materials (SBOM), which lists all the software components used in the device. This helps both manufacturers and healthcare providers quickly identify and fix any vulnerabilities that may arise.

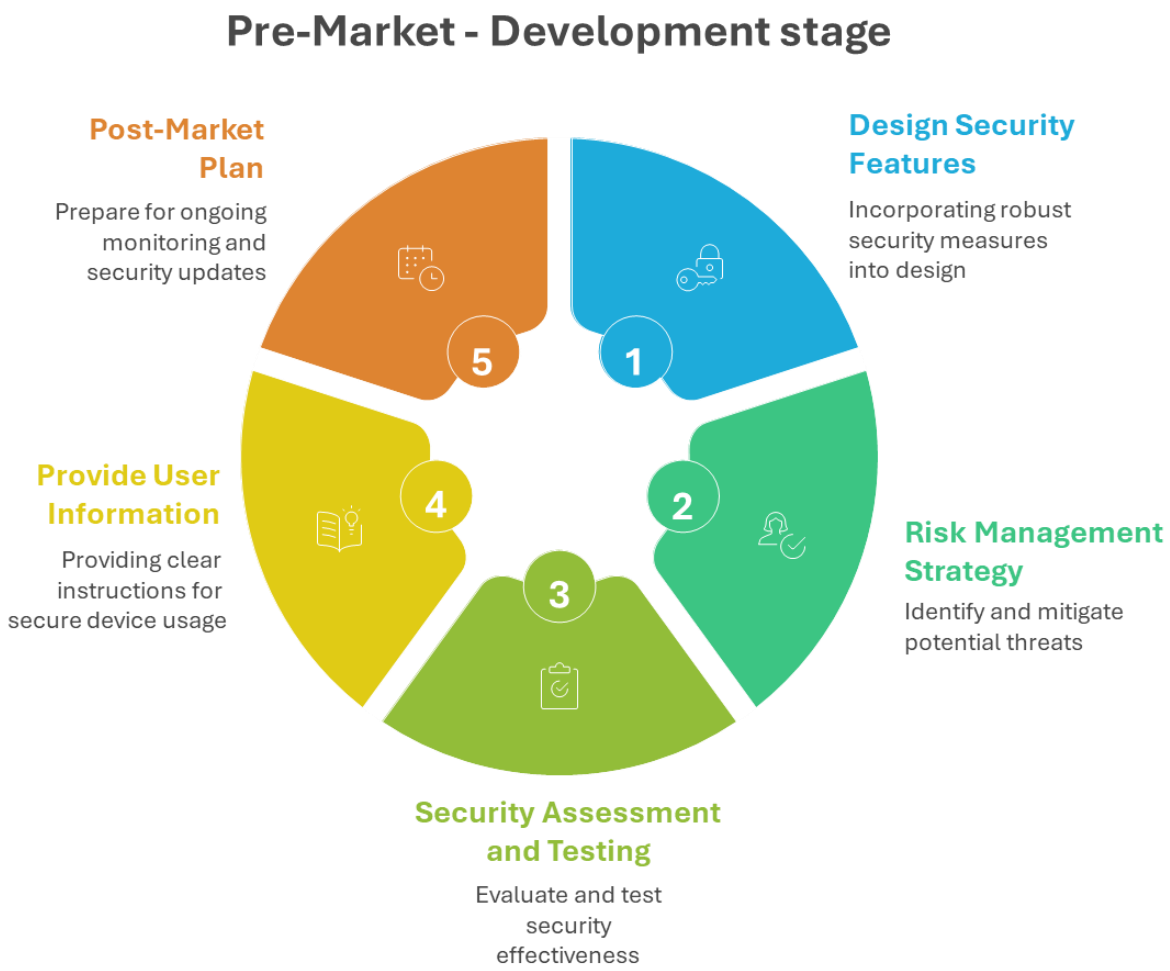

Figure 2: Pre-market elements during the development stage

6.1 Designing Security Features

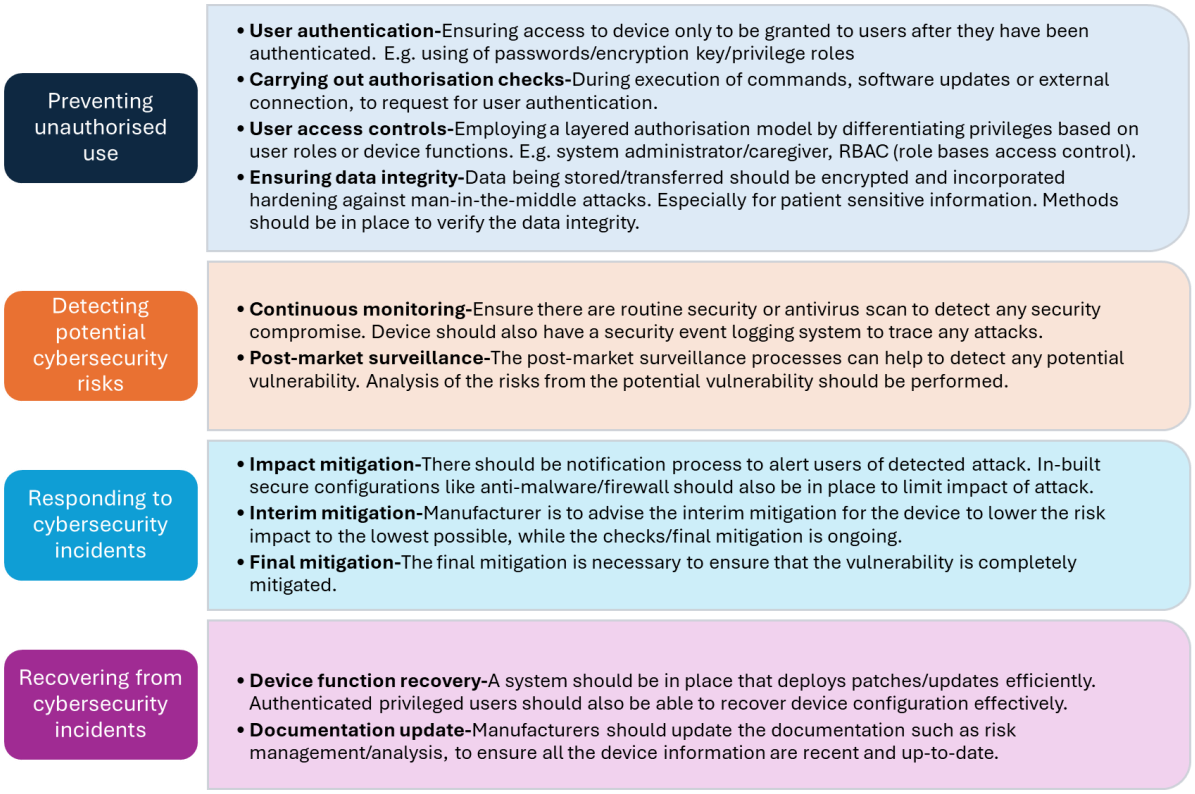

Figure 3: Design considerations for security features

Two important principles, **Secure by Default** and **Secure by Design**, help improve the cybersecurity of systems and applications, including medical devices.

Secure by Default means that a device or system is configured or set up to be as secure as possible right from the start, without needing users to change any settings. This reduces the chance of mistakes or oversights that could lead to security problems.

Secure by Design means building security into the device from the outset of the design process. It involves anticipating possible risks early on and ensuring the device's architecture is robust and resistant to attacks. This helps prevent security issues and reduces the need for costly fixes later.

Both principles are essential for protecting medical devices from cyber threats. Manufacturers are encouraged to include both approaches when designing and developing their products.

6.2 Risk Management Steps

Risks can occur at any stage in a medical device's TPLC. These stages typically include concept and design, manufacturing and supply chain, distribution and installation, clinical use and operation, maintenance and servicing, post-market surveillance, and end-of-life decommissioning or disposal. Sometimes, a risk identified at one stage can be addressed by actions taken at a completely different stage. For example, a software vulnerability discovered during clinical use (post-market) may be mitigated by implementing stronger secure-by-design controls in the next product iteration or by releasing a security patch to existing devices. Because of this interconnected nature, the risk management steps should cover the entire life cycle. In practice, this means the systematic application of risk management principles from the device's initial concept and design all the way through to its End of Life (EOL).

Risk Management Planning

The process begins with the establishment of Risk Management Plan, which formally declares that cybersecurity is within the scope of risk management activities. This plan should define specific criteria for determining the acceptability of risks arising from security threats. Furthermore, it is essential that the team responsible for risk management includes individuals with dedicated cybersecurity expertise, who can properly identify and assess threats that are unique to the digital and networked nature of modern medical devices.

Risk Analysis

During the Risk Analysis phase, the team should identify potential hazards and the foreseeable sequences of events that could lead to harm. In the cybersecurity context, a hazard often stems from compromises to the confidentiality, integrity, or availability of the device, its data, software and functions. These compromises via threats such as malware, unauthorised access, or denial-of-service attacks can create hazardous situations that lead to harm (e.g., patient injury from altered device function, delayed treatment, or incorrect clinical decisions). The risk analysis involves documenting the device's security characteristics, such as its network connectivity, the data it handles

and its software components, to understand its attack surface and potential vulnerabilities.

Following identification, the risk associated with each hazardous situation is to be estimated. This involves determining the potential severity of harm and the probability (or likelihood) of that harm occurring. For example, a ransomware attack that renders a medical device inoperable could lead to a catastrophic outcome for a patient dependent on it. Estimating the probability of a cyberattack could be difficult due to the intentional nature of threats. In such cases, it is recommended to assess exploitability (e.g. Common Vulnerability Scoring System approaches) of known vulnerabilities. If vulnerability is known and exploitable, one should assume it could be targeted and focus the analysis on the severity of the resulting harm.

Risk Evaluation

The Risk Evaluation phase is where formal judgment is made. Each estimated risk is compared against the acceptability criteria established in the risk management plan, often visualised using a risk matrix. This matrix plots severity against probability, with predefined regions for acceptable and unacceptable risks based on the criteria established in the risk management plan. If a risk, such as the remote alteration of an infusion pump's dosage, falls into the unacceptable region, it is evaluated as unacceptable and documented as requiring mitigation. Risks should be reduced as far as possible using the hierarchy of risk controls (see Risk Control below).

Risk Control

When a risk is evaluated as unacceptable, the Risk Control phase is initiated. Risk control measures should be selected and implemented according to the following hierarchy of preference (per ISO 14971):

- Inherent safety by design (e.g., secure boot, code signing, hardened OS);
- Protective measures (e.g., encryption, network segmentation);
- Information for safety (e.g., clear instructions on patch management or limitations).

Examples of effective security controls include the following:

- Authentication & Authorisation: Passwords, role-based access control
- Encryption: Protecting data at rest and in transfer
- Secure Design: Hardening the operating system, code signing, secure boot
- Network Segmentation: Isolating the medical device from non-critical networks
- Patch Management: Having a process to update software to fix vulnerabilities

The goal of each control is to either reduce the likelihood of a successful attack or limit the severity of the harm if an attack occurs.

Evaluation of Residual Risk

After implementing controls, the remaining risk, known as residual risk, should be evaluated to determine whether the security measures have reduced the risk to the predefined acceptable level. As no control is perfect, some residual risk will remain. The team should analyse this remaining risk to confirm that it meets the acceptability criteria and does not introduce new hazards.

If a residual risk is still considered unacceptable after all practicable controls have been applied, a Benefit-Risk Analysis should be performed. The manufacturer should provide a documented justification that the medical benefits of using the medical device for the patient and user outweigh the remaining residual risks.

Continuous Monitoring and Improvement

Cybersecurity risk management is not a one-time effort. It is a continuous process that extends throughout the device's entire life cycle through production and post-production activities. This includes actively monitoring threat intelligence sources for new vulnerabilities, maintaining an incident response plan, and providing security patches to customers. New information gathered from the field should be fed back into the risk management file and may initiate a new cycle of risk analysis and evaluation to help ensure that the device remains safe and secure over time.

6.3 Security Assessment and Testing

Security control verification testing should ensure successful implementation of identified security requirements. Traceability from requirement to verification testing result should ensure that all identified security controls are successfully implemented.

There are several types of cybersecurity testing that manufacturers can conduct to assess the security of their systems and applications. Here are some cybersecurity assessment and testing methods (not exhaustive) that can be considered:

a) Vulnerability Testing

This involves scanning systems for known vulnerabilities and weaknesses, often using automated tools, to identify potential entry points for attackers.

b) Penetration Testing

Penetration testing involves simulating real-world attacks on systems, networks, or applications to identify and exploit vulnerabilities. This helps manufacturers understand their security posture and potential impact of successful attacks.

c) Security Audits

Security audits involve comprehensive reviews of security policies, procedures, and technical controls to ensure compliance with security standards (e.g. TR 67:2018, UL 2900-1, UL 2900-2-1, IEC 81001-5-1, ISO/IEC 27001 and ISO/IEC 27002) and best practices.

d) Security Code Review

This involves manual or automated review of source code to identify security vulnerabilities, such as injection flaws, authentication issues, and other weaknesses.

e) Security Configuration Review

This type of testing assesses the configuration settings of systems, networks, and applications to ensure that they are aligned with security best practices and standards.

There are many ways to test the cybersecurity of medical devices, and each method serves a different purpose. No single approach works for every situation.

Organisations should choose the testing methods that best suit their needs, based on the type of device, how it will be used and the level of risk involved. Devices that carry higher risks may need more thorough and frequent testing. By selecting the most suitable testing method, or a combination of methods, it can better identify and fix security issues, thus helping to keep devices safe and reliable.

Singapore's Cyber Security Agency (CSA) has introduced **the Cybersecurity Labelling Scheme for Medical Devices, known as CLS(MD)**. This scheme encourages manufacturers to build medical devices with stronger security features. For healthcare providers, CLS(MD) offers a clear and tiered label that shows the level of cybersecurity built into a device. This helps them make better-informed choices when selecting devices. As part of good cybersecurity practice, healthcare providers are strongly encouraged to consider the CLS(MD) label as one of the key factors when buying or choosing medical devices. Doing so can help reduce cybersecurity risks within their organisations.

6.4 User Information

It's important to give users clear, complete and easy-to-follow information so they can use the medical device safely and securely. The user manual or instructions for use (IFU) should explain how to set up and use the device, including how to turn on security features. It should also describe any potential cybersecurity risks the device might have and offer tips on how to keep it secure over time.

Users should be given simple security guidelines that show what they can do to protect the device and any personal or medical data it handles. If users face any problems related to security, they should know how to fix them or where to get help. The documentation should clearly explain how to troubleshoot issues and who to contact for support. Contact details for the manufacturer's support or security team should be easy to find, so users can quickly report any security concerns or ask for help.

Instructions should also be provided on how to update the device's software or firmware to ensure that the device is running on the latest secure versions. These updates help fix security problems and keep the device running safely.

The documentation should clearly state any security certifications or standards the device complies with. This helps users feel confident that the device has been tested and meets recognised safety and security requirements.

When it comes to Customer Security Documentation for medical devices, it's essential to provide relevant and easy to understand information to guide users on how to operate the device securely. Manufacturers should also effectively communicate relevant security information when users operate the medical device in its intended operating environment. The following are Customer Security Documentation elements that should be considered:

- Provide users with detailed instructions on the necessary supporting infrastructure requirements to ensure the device operates as intended.
- A detailed explanation of how the device is or can be fortified through secure configurations. These secure configurations may involve endpoint protections such as anti-malware, firewalls/firewall rules, whitelisting, security event parameters, logging parameters, and physical security detection.
- Provide technical instructions, when necessary, for secure network deployment and servicing, along with guidelines for users on how to respond when a cybersecurity vulnerability or incident is detected.
- An explanation of how the device or supporting systems will alert the user when anomalous conditions are detected, if feasible. Types of security events may include configuration changes, network anomalies, login attempts, and anomalous traffic.
- An explanation of the methods for retaining and recovering device configuration by an authenticated privileged user.
- An outline of the security risks and consequences associated with changes to the security configuration or the use of the environment.
- A description of the systematic procedures for authorised users to download and install updates from the manufacturer.
- Information regarding the End of Support (EOS) for device cybersecurity.
- A Software Bill of Materials (SBOM).

Because cybersecurity information may reveal potential weaknesses in a medical device, it is important to handle it carefully. Manufacturers should establish secure communication channels to share such sensitive information with users. This ensures that details about vulnerabilities are protected and only accessible to authorised parties, helping to prevent misuse and maintain trust.

6.5 Post-Market Plan

Post-Market Plan - Developing a plan for on-going post-market activities, including monitoring, timely detecting, and addressing any security issues or emerging threats that may arise after the device has entered the market.

Key considerations for the post-market plan include:

1. Post-market Vigilance
2. Vulnerability Disclosure
3. Patching and Updates
4. Recovery
5. Information sharing

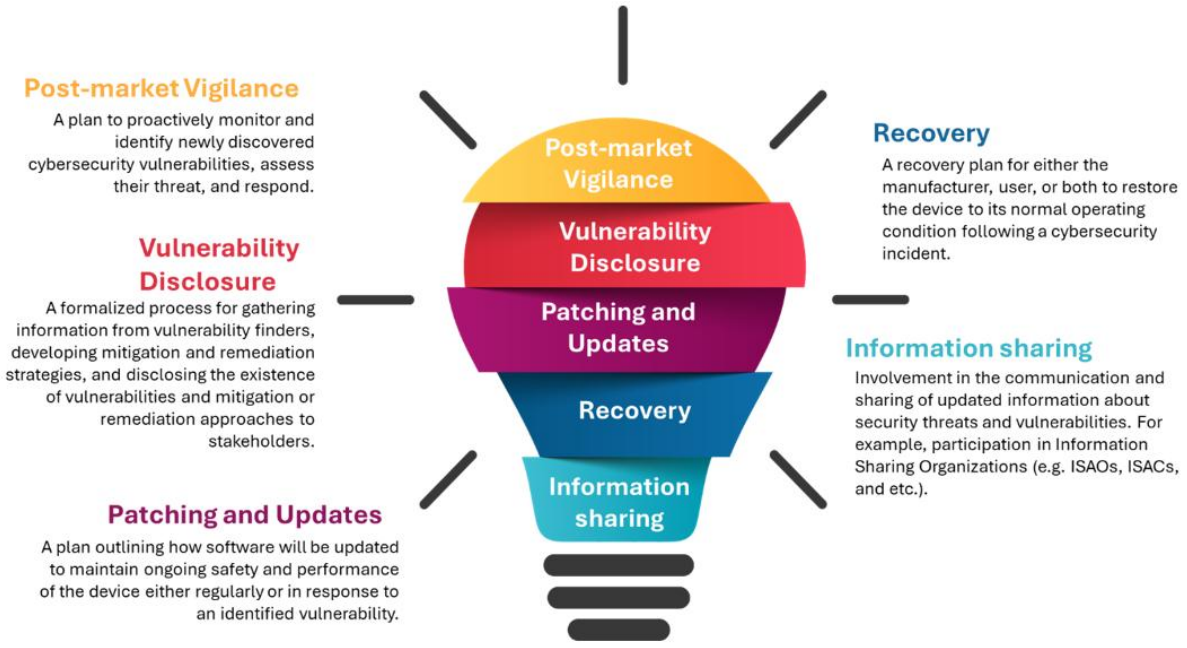

Figure 4: Key considerations for the post-market plan.

When manufacturers take care of these post-market aspects, they help strengthen the cybersecurity of their medical devices. This also supports the overall safety and reliability of the healthcare technology and services that patients and providers rely on.

6.6 Software Bill of Materials (SBOM)

The Software Bill of Materials, or SBOM, is a concept introduced in 2018 by the U.S. National Telecommunications and Information Administration (NTIA) to improve transparency in software. An SBOM is essentially a detailed list of all the software components used in a device or application. This includes open-source tools, third-party software, libraries and any other parts that make up the system. By knowing what's inside the software, manufacturers and users can better understand potential risks and manage cybersecurity more effectively.

Using an SBOM has become more important in today's cybersecurity landscape. It helps organisations keep track of all the software parts used in their systems. This is crucial for spotting and fixing any weaknesses that might exist in the software supply chain, making the overall system more secure and reliable.

For medical devices, having an SBOM is especially important. It helps manufacturers, users, and healthcare providers understand what software components are inside the device and what security risks might be linked to them. An SBOM also makes it easier to track software updates and patches, which supports a safer and more reliable medical device environment.

The following are the SBOM key elements:

- Author name - denotes the entity (such as an individual, organisation, or similar) responsible for producing the SBOM file.
- Timestamp - a record of the date and time when the SBOM data was assembled.
- Software component vendor (supplier) - the entity responsible for creating, defining, and identifying components. The software component vendor name should typically refer to the legal business name used for the commercial software.

- Software component name - the designation given to a software unit by the original supplier.
- Software component version - the identifier assigned by the supplier to denote a change in the software from a previous version.
- Unique Identifier – identifiers used to recognise a component or function as a look-up key for relevant databases.
- Dependency Relationship - explains how an upstream component X is related to software Y.

The following use cases demonstrate how SBOMs play a crucial role in enabling organisations to respond to cybersecurity incidents, assess risks, communicate with vendors, plan remediation efforts, and maintain compliance within the complex and rapidly evolving healthcare technology ecosystems.

6.6.1 Use Case #1: Medical Device Manufacturer's Security Compliance

Scenario:

ABC Medical Devices Pte Ltd is a manufacturer of advanced medical imaging equipment. They are committed to ensure the security and integrity of their devices to protect patient data and maintain the reliability of their products.

Use of SBOM:

ABC Medical Devices utilises SBOM as part of their cybersecurity and risk management strategy. When developing their medical imaging equipment, they maintain a comprehensive SBOM that lists all the software components, libraries, and dependencies used in building the device's software.

Transparency and Compliance:

The SBOM allows ABC Medical Devices to maintain transparency and compliance with regulatory requirements related to software components and security standards. It provides a clear overview of all the software elements used in their medical devices, including open-source and third-party components.

Vulnerability Management:

By maintaining an up-to-date SBOM, ABC Medical Devices can proactively monitor and manage potential vulnerabilities associated with the software components used in their devices. They can stay informed about security advisories, patches, and updates for the components listed in the SBOM, and thus update the users promptly with the information.

Supply Chain Security:

The SBOM enables ABC Medical Devices to assess the security posture of their software supply chain. They can evaluate the security practices of their software vendors and ensure that the components used in their devices meet the necessary security standards.

Incident Response and Remediation:

In the event of a security incident or vulnerability disclosure related to a software component, the SBOM allows ABC Medical Devices to quickly identify the affected devices and take appropriate remediation actions, such as applying patches or updates to mitigate the risk.

Overall, the use of SBOM empowers ABC Medical Devices to maintain a secure and compliant software supply chain, proactively manage vulnerabilities, and respond effectively to security incidents, thereby enhancing the cybersecurity of their medical imaging equipment.

Without SBOM:

- ABC Medical Devices Pte Ltd must manually inspect the codebase or rely on developer memory in the event of security patch management.
- Delays in patching increase exposure and risk of vulnerability.
- Communication with customers is slower and less precise.

6.6.2 Use Case #2: Cybersecurity Incident Response and Remediation

Scenario:

XYZ Healthcare is a large hospital network that relies on a variety of medical devices and software systems to deliver patient care. They prioritise cybersecurity to protect patient data and ensure the reliability of their healthcare technology infrastructure.

Use of SBOM:

XYZ Healthcare leverages SBOM as a critical component of their cybersecurity incident response and remediation strategy. They require SBOMs from their medical device manufacturers, IT and software vendors to ensure transparency and visibility into the software components used in the devices and systems deployed across their network. This information is also part of the requirements in the procurement process of XYZ Healthcare.

Incident Response:

In the event of a cybersecurity incident or the discovery of a software vulnerability, XYZ Healthcare utilises the SBOMs provided by their vendors to quickly identify the affected software components and devices within their network.

Risk Assessment:

The SBOMs enable XYZ Healthcare to conduct rapid risk assessments by understanding the software supply chain dependencies and identifying potential security implications associated with the affected components.

Vendor Communication:

By using the SBOMs, XYZ Healthcare can effectively communicate with their device manufacturers, IT and software vendors to request relevant security patches, updates, or mitigation strategies to address the identified vulnerabilities.

Remediation Planning:

The SBOMs serve as a foundation for developing targeted remediation plans, allowing XYZ Healthcare to prioritise and apply security updates to the affected devices and software components in a timely manner. XYZ Healthcare should liaise with the manufacturer to ensure the implementation of appropriate interim and final measures.

Compliance and Reporting:

SBOMs support the compliance efforts by providing a clear record of the software components and their associated security status, which is essential to demonstrate due diligence in managing cybersecurity incidents.

By leveraging SBOMs in their incident response and remediation processes, XYZ Healthcare can effectively manage and mitigate cybersecurity risks, ensuring the security and integrity of their healthcare technology infrastructure.

Without SBOM:

- XYZ Healthcare has no visibility of the software components.
- It takes longer to assess exposure and respond to cybersecurity threats.
- The device remains vulnerable for a longer period, increasing patient safety risks.

6.7 Additional consideration - Devices with Artificial Intelligence (AI)

AI is becoming an important part of medical devices, supporting tasks such as diagnosis, prediction of disease risks, and workflow improvement. While AI can make healthcare more efficient and cost-effective, it also introduces new risks. If an AI-enabled medical device is attacked or compromised, it could lead to incorrect diagnoses, treatment errors, or serious patient harm. With the rise of Generative AI, additional threats have emerged, such as prompt injection, false outputs (hallucinations), misinformation, and accidental data leakage. These risks should be addressed alongside traditional cybersecurity threats to help keep AI-enabled medical devices safe.

To build safe and secure AI systems in medical devices, manufacturers and healthcare providers should focus on key areas throughout the AI development cycle. This includes securing the AI model design, protecting the AI supply chain during development, ensuring safe deployment, and maintaining strong security during operation and updates after deployment.

It’s also important to protect patient data, regularly check AI outputs for accuracy and be transparent about how AI-generated content is used. On-going security checks and updates are essential to stay ahead of new and evolving threats.

In addition, AI developers have a responsibility to ensure their systems are safe before releasing them. This means thoroughly testing the system for security risks. Once released, they should clearly explain any known limitations so users understand what the system can and cannot do. Before using the AI system in real-world settings, users should carefully consider its benefits and drawbacks, including any limitations that might affect its performance or safety.

7. POST-MARKET STAGES

Connected medical devices placed on the Singapore market go through three post-market stages: Support, Limited Support, and End of Support. The recommendations in this section apply to devices newly supplied in Singapore and devices already installed and in use. At each stage, manufacturers, product registrants, importers, local authorised representatives, and healthcare providers have different responsibilities. Healthcare provider responsibilities commence from the **Support stage**, and operational responsibility increases as devices approach End of Life (EOL) and End of Support (EOS).

7.1 Support stage

During the **Support stage**, manufacturers should provide full cybersecurity support to healthcare providers, including software patches and updates. Product registrants, importers, and local authorised representatives should facilitate the timely provision of support and cybersecurity information to users in Singapore. Users should have access to sufficient information to assess the device's cybersecurity.

7.1.1 Procurement and installation

Manufacturers should provide:

Product Security Documentation (such as SBOM and identified security gaps) to help users manage risks during procurement and deployment.

Product Life Cycle Documentation (including cybersecurity EOL and EOS dates when available) covering:

- Device operating system and version
- Known software issues in each version
- Software components
- Required ports and services
- Firewall rules for device isolation
- Expected service change dates
- Available maintenance after changes
- Anti-malware and security scanning capabilities
- Security logging capabilities

- Backup and restore procedures
- Vulnerability notification methods
- Administrative accounts and privilege management
- Additional compensating controls (alternative security measures when standard controls are absent)

Manufacturers should clearly communicate the schedule of service changes and available maintenance, including for third-party components. Product registrants, importers, and local authorised representatives should support timely communication of this information to affected users in Singapore.

Important: Share sensitive information through secure, trusted channels to prevent compromise and reduce risk exposure.

7.1.2 When device is in use

Manufacturers and healthcare providers should maintain strong communication to enable prompt support when vulnerabilities emerge. Product registrants, importers, and local authorised representatives should facilitate the flow of relevant cybersecurity information and actions in Singapore.

Manufacturers are recommended to:

- Update Product Security and Product Life Cycle Documentation as changes occur
- Provide Vulnerability and Patching Information promptly, including available mitigations
- Monitor software components (operating systems, third-party components) to ensure adequate support
    - For efficient monitoring, include:
        - Expected EOL/EOS dates
        - Software Bill of Materials (SBOM)
        - Software upgrade options
        - Software change schedule
        - Maintenance schedule

        - Risk analysis documentation (available mitigations, potential new risks)
- Inform healthcare providers when components reach EOL/EOS

Both parties are recommended to:

- Conduct post-market surveillance, including:
    - Continuous monitoring for security threats and anomalies
    - Collecting and reviewing all complaints (internal and external)
    - Reporting adverse events and field safety corrective actions to regulatory authorities
    - Active risk management to address security issues promptly

- Share cybersecurity awareness about potential threats and best practices to ensure safe and secure device usage.

- Manufacturers and healthcare providers should establish a vulnerability management process to review and assess vulnerabilities. Key principles include:
    1. **Apply software updates when available** to prevent exposure to vulnerabilities
    2. **Identify assets** by maintaining a list of components with relevant information (version, supplier, EOL/EOS dates)
    3. **Triage and prioritise critical updates** to address the most serious risks first
    4. **Document justification** when updates are not implemented, including risk assessment
    5. **Verify and regularly review the system** to identify new threats and monitor current vulnerabilities

Healthcare providers should:

- Comply with the Cyber & Data Security Guidelines for Healthcare Providers issued by the Ministry of Health, Singapore, in accordance with the Health Information Act 2026.

7.1.3 Transfer of responsibility

The transition from Support to Limited Support marks a gradual shift in operational responsibilities from manufacturers to healthcare providers. As devices approach EOL and EOS, manufacturer support decreases while healthcare providers' responsibility for managing the risks of continued use increases. Product registrants, importers, and local authorised representatives should support advance communication, transition planning, and access to relevant product security information in Singapore.

Recommended timeline: Begin transition approximately 2 to 3 years before EOS (may vary based on device complexity and criticality).

Manufacturers should inform healthcare providers of the expected EOS date early to allow sufficient time for evaluation, planning, and budgeting for device retirement or replacement. The transfer of operational responsibility at EOS applies to the continued use of devices that were previously placed on the Singapore market with an adequate manufacturer-supported cybersecurity life cycle; it should not be interpreted as a general basis for shifting manufacturer life cycle responsibilities to healthcare providers before EOS.

During transition:

Manufacturers should:	**Healthcare providers should:**
Provide updated Product Security Documentation	Assess your ability to manage the device from cybersecurity and clinical perspectives
Provide information on configurable security options at EOL/EOS (software only, partial software and hardware, or complete replacement)	Identify possible third-party support and additional resources needed
Inform users about configurable security options	Assess the risks of continuing device usage and necessary management measures
	Assess potential device replacement opportunities

7.2 Limited Support stage (Between EOL and EOS)

During Limited Support, manufacturers and healthcare providers should maintain close communication. Product registrants, importers, and local authorised

representatives should facilitate communication with users in Singapore. Relevant information about the product, potential risks, mitigations, remaining support, and replacement options should be readily available.

Manufacturers are recommended to:

- Inform healthcare providers about the reduction in support to "Limited Support"
- Provide a timeline until EOS
- Alert users about parts no longer supported
- Detail available software updates
- Recommend compensating controls (alternative risk control measures)

Healthcare providers are recommended to evaluate whether to continue using the device by considering:

- **Risk of usage:** Security risks due to limited manufacturer support
- **Usability:** Whether limited features remain suitable for patients
- **Support resources:** Resources required to maintain the device (compensating controls, maintenance costs)
- **Patient impact:** Potential impact if the device becomes unusable

If purchasing a new device, account for the potential gap between current device EOS and new device availability. Begin decision-making and planning approximately 2 to 3 years before EOS.

7.3 End of Support stage

At EOS, the healthcare provider assumes primary operational responsibility for managing the cybersecurity risks associated with continued use of the device without active manufacturer support. This transfer applies only to devices that were previously placed on the Singapore market with an adequate manufacturer-supported cybersecurity life cycle. It does not remove any continuing responsibilities that may apply to the manufacturer, product registrant, importer, or local authorised representative, including communicating known safety risks, supporting appropriate safety actions, and meeting applicable regulatory reporting obligations.

Manufacturers should:

- Provide all necessary product security information to healthcare providers and, where relevant, to product registrants, importers, and local authorised representatives supporting users in Singapore
- Inform affected users and, where appropriate, the public about the device's transition to EOS through security bulletins, website updates, or other suitable communication channels
- Continue to communicate known cybersecurity-related patient safety risks and support applicable post-market safety and regulatory reporting activities, as appropriate.

If healthcare providers continue using the device beyond EOS, they should:

- Implement a strong cybersecurity programme with allocated resources
- Conduct risk assessments weighing cybersecurity risks against clinical benefits
- Establish a robust inventory management system including a vulnerability database for third-party components
- Enhance risk measures through compensating controls (limiting physical access, removing remote access, using firewalls, network segregation or isolation)
- Periodically evaluate alternative devices and re-evaluate the decision to continue use

Staff should be trained on safe and secure device use and on how to identify and respond to unusual device behaviour.

7.4 Summary

The post-market stage has three phases:

1. **Support Stage:** Manufacturer provides active maintenance and regular updates, including continuous vulnerability monitoring, timely security patches, technical support, on-going risk assessments, and cybersecurity improvements.

2. **Limited Support Stage:** Update frequency decreases, support focuses on critical security issues, manufacturer encourages migration to newer versions, and legacy systems may require additional security measures.

3. **End of Support Stage:** The manufacturer no longer provides active support, and the healthcare provider assumes primary operational responsibility for risks associated with continued use. Clear EOS communication, secure decommissioning guidance, management strategies for legacy devices, and appropriate compensating controls remain important. Any continuing manufacturer or Singapore supply-chain responsibilities, including communication of known safety risks and applicable regulatory reporting, should still be fulfilled.

Throughout all stages, effective cybersecurity management requires collaboration between manufacturers, healthcare providers, and cybersecurity experts to maintain device security and integrity throughout the entire life cycle.

The following figure provides an overview of cybersecurity best practices throughout the medical device TPLC.

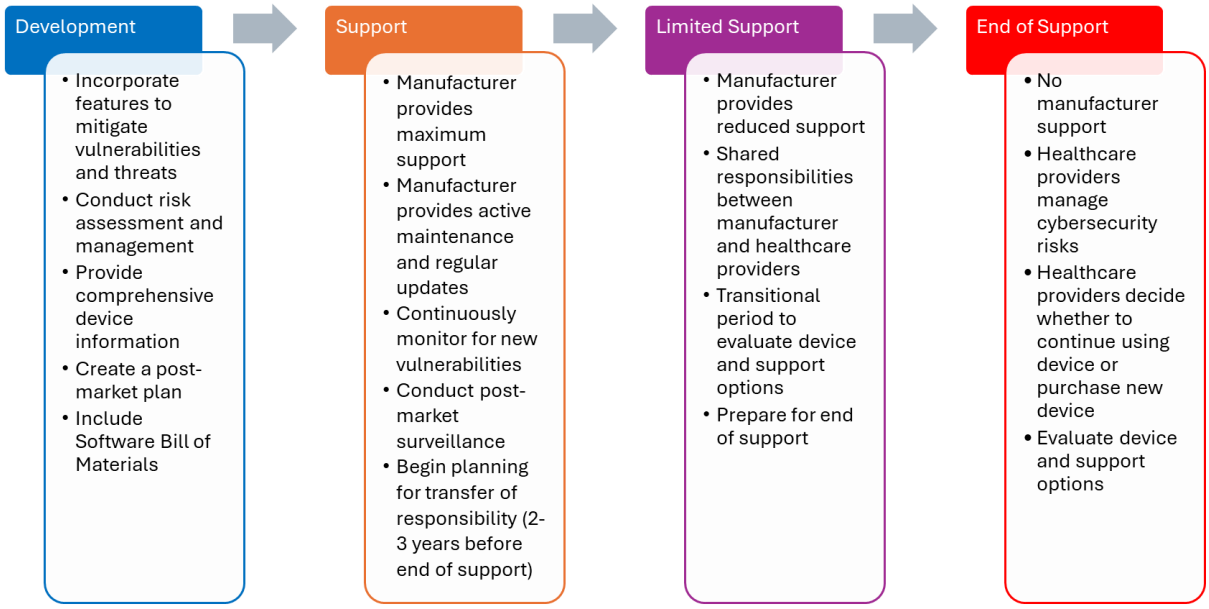

Figure 5: Overview of the cybersecurity best practices in the TPLC of the medical device

8. CONCLUSION

Medical device cybersecurity is constantly evolving. Manufacturers, product registrants, importers, local authorised representatives, and healthcare providers should remain vigilant and adapt to new threats throughout the device life cycle.

It is critical that security is integrated from the outset of device development. Manufacturers should implement robust risk management strategies, conduct thorough security testing, and provide transparent documentation including Software Bill of Materials (SBOM). These steps are essential for creating secure medical devices that can withstand evolving cyber threats.

Cybersecurity remains an on-going responsibility across all post-market stages for connected medical devices placed on the Singapore market: Support, Limited Support, and End of Support. As threats evolve and new vulnerabilities emerge, continuous monitoring, timely updates, and proactive risk management are critical. The transfer of operational responsibility at EOS concerns the continued use of previously supported devices and should be accompanied by careful transition planning and appropriate risk mitigation.

Medical device cybersecurity is a shared responsibility requiring on-going communication among manufacturers, product registrants, importers, local authorised representatives, and healthcare providers. Applying these best practices to connected medical devices placed on the Singapore market can support a safer healthcare ecosystem that protects device performance, patient safety, and cybersecurity.

9. REFERENCES

[1] IMDRF/CYBER WG/N60FINAL:2020 Principles and Practices for Medical Device Cybersecurity

[2] IMDRF/CYBER WG/N70FINAL:2023 Principles and Practices for the Cybersecurity of Legacy Medical Devices

[3] IMDRF/CYBER WG/N73FINAL:2023 Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity

[4] HSA Regulatory Guidelines for Software Medical Devices – A Life Cycle Approach

[5] Shifting the Balance of Cybersecurity Risk Principles and Approaches for Secure by Design Software [https://www.cisa.gov/resources-tools/resources/secure-by-design]

[6] Guidelines for secure AI system development by UK National Cyber Security Centre (NCSC), the US Cybersecurity and Infrastructure Security Agency (CISA) [https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development]

[7] UK National Cyber Security Centre - Vulnerability management [https://www.ncsc.gov.uk/collection/vulnerability-management]

[8] US FDA Guidance: Cybersecurity in Medical Devices-Quality System Considerations and Content of Premarket Submissions

[9] MDCG 2019-16 Guidance on Cybersecurity for medical devices

[10] Cybersecurity Labelling Scheme for Medical Devices, CLS(MD) [https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/cls-md/publications]

[11] MOH Cyber & Data Security Guidelines for Healthcare Providers [https://www.healthinfo.gov.sg/files/MOH_Cir_No_85_2023_04Dec2023_Cyber_and_Data_Security_Guidelines_for_Healthcare_Providers_Annex_A.pdf]

HEALTH SCIENCES AUTHORITY

Health Products Regulation Group
Blood Services Group
Applied Sciences Group

www.hsa.gov.sg

Contact Information:

Medical Devices Cluster
Health Products Regulation Group
Health Sciences Authority

11 Biopolis Way, #11-03 Helios
Singapore 138667
www.hsa.gov.sg

HSA
Health Sciences Authority