Best Practices Guide for Medical Device Cybersecurity

Medical Devices Cluster
Health Products Regulation Group
Health Sciences Authority, Singapore

Contents

1 Introduction

In the rapidly evolving landscape of healthcare technology, the cybersecurity of medical devices has become a critical concern. As these devices become increasingly interconnected and software-dependent, they offer immense benefits to patient care but also present new vulnerabilities to cyber threats. Such vulnerabilities, if exploited, may result in patient harm, delays in treatment, etc.

This document is intended for medical device manufacturers and healthcare providers. It provides recommendations on cybersecurity best practices for medical devices, focusing on both pre-market and post-market stages of the device's total product lifecycle (TPLC).

The pre-market stage focuses on the development phase, where cybersecurity measures are integrated into the device during the development phase. This crucial stage encompasses designing security features (i.e. Secure by Design), developing risk management strategies, conducting thorough security testing, preparing user information and documentation, developing a post-market cybersecurity plan, and creating a Software Bill of Materials (SBOM).

The post-market stage addresses cybersecurity risks throughout the device's operational life. This stage is further divided into three sub-stages: the Support Stage, the Limited Support Stage, and the End of Support Stage. During the Support Stage, active maintenance and updates are provided to ensure the device remains secure against emerging threats. The Limited Support Stage involves reduced but continued security support, while the End of Support Stage focuses on managing cybersecurity risks for legacy devices that are no longer actively supported.

By adhering to these best practices across both premarket and post-market stages, manufacturers and healthcare providers can work together to enhance the security posture of medical devices, protect patient safety, and maintain the integrity of healthcare systems. As the field of medical device cybersecurity continues to evolve, it is crucial to stay informed about emerging threats and adapt the applicable strategies accordingly.

2 Scope

This document is not intended to provide information on regulatory requirements, but rather offers best practices recommendations and considerations on medical device cybersecurity throughout the Total Product Life Cycle (TPLC).

The scope of this document is to provide recommendations to all medical device manufacturers and healthcare providers on general cybersecurity principles to ensure medical devices are secure throughout their lifecycle, from device development to the end-of-support phase.

3 Definitions

Asset: physical or digital entity that has value to an individual, an organization or a government.

Attack: attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Availability: property of being accessible and usable on demand by an authorized entity.

Confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Cybersecurity: a state where information and systems are protected from unauthorized 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.

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.

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.

Exploit: defined way to breach the security of information systems through vulnerability.

Integrity: property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored.

Patient Harm: physical injury or damage to the health of patients.

Security testing: type of testing conducted to evaluate the degree to which a test item, and associated data and information, are protected so that unauthorized persons or systems cannot use, read, or modify them, and authorized persons or systems are not denied access to them.

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

Threat: potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

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

Vulnerability: weakness of an asset or control that can be exploited by one or more threats.

4 General Principles

4.1 Shared Responsibilities

The cybersecurity of medical devices is a shared responsibility between device manufacturers and healthcare providers. Both parties need to understand their roles, responsibilities and collaborate closely with each other to continuously monitor, assess, mitigate, communicate and respond to potential cybersecurity risks and threats throughout the device's life cycle.

In addition, medical devices manufacturers are encouraged to take ownership of improving the security outcomes and evolving devices accordingly. The burden of security should not fall solely on the healthcare providers.

Although technical subject matter expertise is crucial for device security, senior management in the manufacturers and healthcare organizations are the primary decision-makers for implementing changes within an organization. Hence, senior management plays an important role in ensuring the safety of the device during its life cycle.

4.2 Transparency and Communication

Cybersecurity information sharing is a foundational principle in the TPLC approach to ensuring the safety and security of medical devices. Active participation, timely sharing of information and coordinated vulnerability disclosure between the manufacturers and healthcare providers are the encouraged best practices.

The active engagement between the manufacturers and healthcare providers will increase the awareness and allows for timely and appropriate planning at each stage of TPLC of the medical device. There should be appropriate channels available to ensure the accessibility of the required information for the manufacturers and healthcare providers.

4.3 Secure by Design

Secure by design is a fundamental principle in cybersecurity that emphasises building security into systems and software at the development phase. This approach involves considering potential threats and vulnerabilities at every stage of the development process, from initial planning to implementation and maintenance.

By integrating security measures into the core architecture and design of a medical device, it will result in a more robust and resilient medical devices that are inherently resistant to cyberattacks. It will help to enhance the overall security of the medical device during its life cycle and reduces the need for costly retrofitting and patch management in the long run.

5 Overview of Total Product Life Cycle Framework (TPLC)

The risks associated with the cybersecurity threats and vulnerabilities need to be considered throughout the Total Product Life Cycle (TPLC) of the medical device. The TPLC approach will allow medical device manufacturers and healthcare providers to manage and adapt to the rapid changes of the medical devices. The aspects involved in TPLC include (but not limited to) design control, shared responsibilities between manufacturers and healthcare providers, risk management at each stage, etc.

The TPLC consists of different stages, i.e. Development, Support, Limited Support and End of Support. It is crucial that risk management is applied at each stage of the TPLC of the medical device. The final two stages of TPLC signals the End of Life (EOL) and End of Support (EOS) for the medical devices. EOL refers to the end of the projected useful life of the medical device and thus only limited support from the manufacturer will be available. On the other hand, at the EOS stage, no further support should be expected from the manufacturer and thus the management and responsibility of the device should solely be performed by the healthcare providers. It is therefore crucial for both the manufacturers and healthcare providers to work together to ensure the medical device can be reasonably protected against the cybersecurity threats.

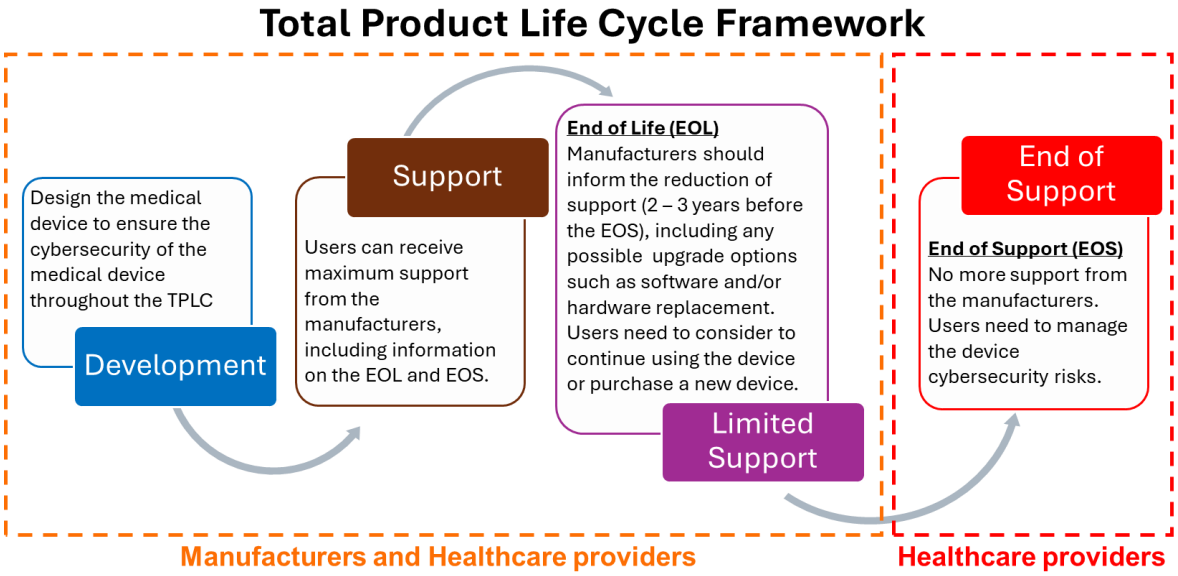

Figure 1: Total Product Life Cycle Framework

The cybersecurity considerations at each stage of TPLC will be discussed in more details in the following sections.

6 Pre-market – Development stage

It is important for medical devices manufacturers to prioritise medical device cybersecurity throughout the entire product life cycle. However, there are specific pre-market elements that should be considered during the development stage to ensure the security of the medical device throughout the TPLC. These include (i) Designing Security Features, (ii) Risk Management Strategies, (iii) Security Testing, (iv) User Information, and (v) Post-Market Plan. In addition to the above elements, manufacturers should consider preparing a Software Bill of Materials (SBOM) to allow both themselves and healthcare providers to have an oversight on the software components used in the device, thus enabling prompt assessment, identification and remediation of any potential vulnerabilities.

6.1 Designing Security Features

Designing Security Features - Incorporating security features into the product design to mitigate potential vulnerabilities and threats. These are some possible design considerations:

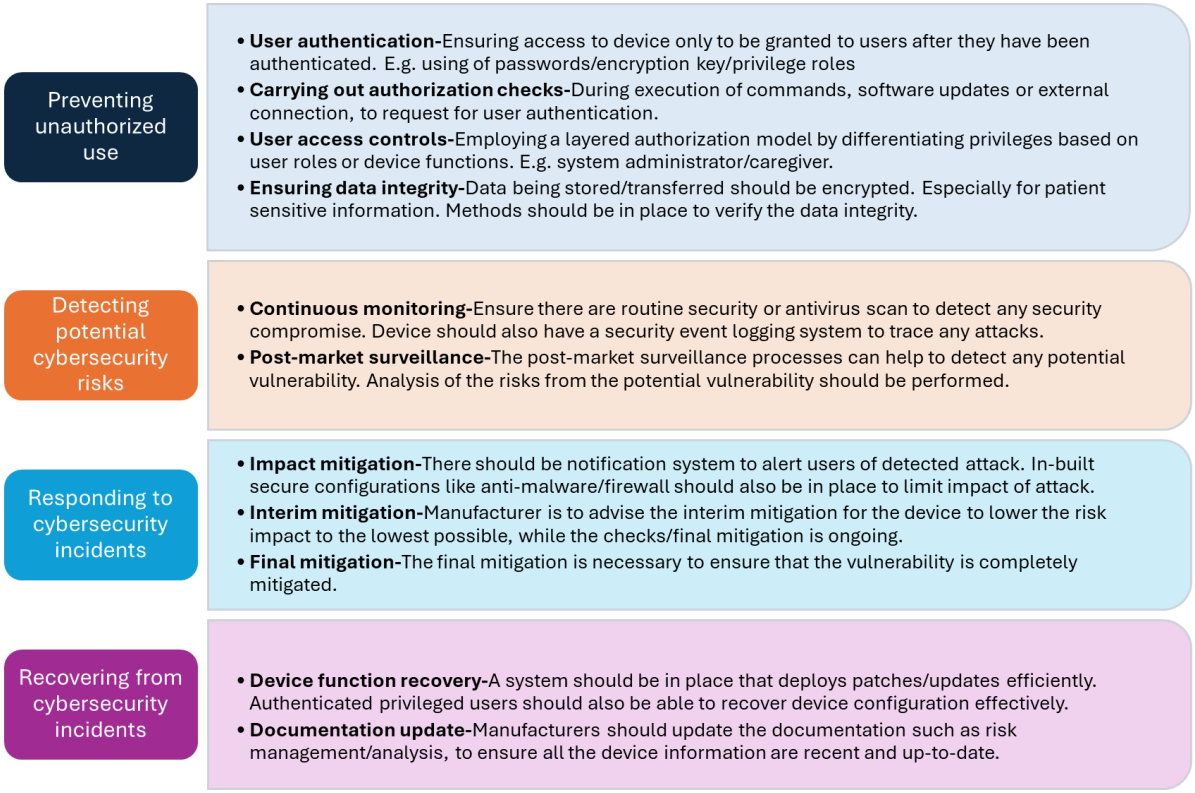

Figure 2: Design considerations for security features

Secure by default and **Secure by design** are two important principles that aim to enhance the security of systems and applications:

a) Secure by default
Secure by default refers to the principle of configuring systems and applications to be as secure as possible out of the box, without requiring additional user intervention. The main focus of secure by default is to ensure that the initial configuration of a system or application prioritises security, thereby reducing the risk of misconfiguration leading to security vulnerabilities. This approach aims to minimize the potential for oversight or human error in configuring security settings, thereby enhancing the overall security posture of the system.

b) Secure by design
Secure by design refers to the approach of integrating security measures and considerations into the design and architecture of a system or application from the outset. The primary focus of secure by design is to proactively identify and address potential security vulnerabilities during the design phase, rather than as an afterthought. As a result, this creates systems that are inherently secure, reducing the likelihood of security breaches and the need for extensive retroactive security measures.

Both principles are crucial for strengthening cybersecurity and mitigating potential risks. Hence, medical devices manufacturers are recommended to integrate both principles into the product design and development processes.

6.2 Risk Management Strategies

Risk Management Strategies - Applying accepted risk management strategies to identify, analyse, assess, and mitigate cybersecurity risks associated with the device. Here are some of the key strategies of the cybersecurity risk assessment and planning that medical device manufacturers and healthcare providers need to consider:

a) Risk Assessment

- **Identifying Assets** - The first step is to identify all the assets, including medical devices, software and data, that are part of the intended use environment.

- **Threat Identification** - Assess the potential threats and vulnerabilities that could impact the confidentiality, integrity, and availability of the medical devices and associated data.

- **Vulnerability Analysis** - Evaluate the vulnerabilities present in the devices, including outdated software, weak authentication mechanisms and potential points of entry for attackers.

  Vulnerability scoring is a method used to assess and quantify the severity and potential impact of security vulnerabilities in systems, applications, or devices. It provides a standardised way to prioritise and address vulnerabilities based on their characteristics and potential risk they pose to the device. There are several common vulnerability scoring systems used in the cybersecurity industry. Two of the most widely used are the **Common Vulnerability Scoring System (CVSS)** and the **Common Weakness Scoring System (CWSS)**.

- **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.

- **Common Weakness Scoring System (CWSS):**
  CWSS focuses on scoring the inherent weaknesses in software, rather than specific vulnerabilities. It aims to quantify the severity of common weaknesses that can lead to vulnerabilities. CWSS considers factors such as the prevalence of the weakness, the potential impact of exploitation, and the ease of detection and remediation. CWSS provides a numerical score to represent the severity of a weakness, allowing organizations to prioritise efforts to address common weaknesses in their software development processes.

  In addition to these standardized scoring systems, organizations may also develop their own internal vulnerability scoring methodologies tailored to their specific needs and risk profiles. These scoring systems often take into account organizational context, industry-specific threats and the potential impact of vulnerabilities on critical assets.

- **Impact Analysis** - Determine the potential impact of a cybersecurity breach on patient safety, data integrity, and healthcare operations. The manufacturers should have a process in place to assess the impact from the cybersecurity vulnerability. For example, manufacturers using a scoring system (e.g. CVSS and CWSS discussed above) to assess the vulnerability and thus determine the need for and urgency of the response.

b) Risk Management

Risk analysis should prioritise evaluating the potential harm to patients/users by taking into account the following: 1) how easily the cybersecurity vulnerability can be exploited, and 2) the severity of patient harm if the vulnerability were to be exploited. Additionally, these analyses should consider compensating controls and risk mitigation strategies.

- **Risk Mitigation** - Develop strategies to mitigate identified risks, such as implementing security controls, patching vulnerabilities, and enhancing access controls.

- **Residual Risk Analysis** - Assess the remaining risks after implementing mitigation measures and determine if they are acceptable or if further action is required.

- **Risk Communication** - Communicate the identified risks with transparency and mitigation strategies to relevant stakeholders, including healthcare providers, device manufacturers and regulatory authorities.

c) Security Plan Development

- **Security Controls Implementation** - Develop and implement security controls to protect medical devices and associated systems from cyber threats. This may include encryption, access controls, intrusion detection systems, and secure software development practices.

- **Incident Response Planning** - Develop a comprehensive incident response plan to address cybersecurity incidents, including procedures for detecting, responding to, and recovering from security breaches.

- **Regulatory Compliance** - Ensure that the security plan aligns with relevant regulatory requirements or other relevant regulatory bodies in different countries.

d) Continuous Monitoring and Improvement

- **Ongoing Assessment** - Continuously monitor the security posture of medical devices and associated systems to identify new risks and vulnerabilities.

- **Security Training** - Provide training to healthcare staff on cybersecurity best practices and the safe use of medical devices to minimize the risk of human error leading to security incidents.

- **Feedback Loop** - Establish an effective feedback loop to incorporate lessons learned from security incidents and near-misses into the risk assessment and planning process.

On top of the recommended strategies above, the cybersecurity risk management process is complementary to and can be integrated as part of ISO 14971 standard - Application of risk management process for medical devices.

6.3 Security Testing

Security Testing - Conducting thorough security testing to identify and address any potential weaknesses or vulnerabilities in the device's security measures.

There are several types of cybersecurity testing that manufacturers can conduct to assess the security of their systems and applications. Here are some common cybersecurity testing methods that can be considered:

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

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

c) Security Audits
Security audits involve comprehensive reviews of an organization's security policies, procedures, and technical controls to ensure compliance with security standards (e.g. TR 67:2018, UL 2900-1, UL 2900-2-1) 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.

f) Security Awareness Training and Testing
This involves educating employees on periodic basis (e.g. monthly, bimonthly or quarterly) about security best practices and conducting simulated phishing attacks or other tests to assess their awareness and response to potential security threats.

g) Red Team vs. Blue Team Exercises
Red team exercises involve simulating real-world attacks to test an organization's defences, while blue team exercises involve defenders responding to and mitigating these simulated attacks.

h) Incident Response Testing
This involves simulating security incidents to test an organization's incident response capabilities, including detection, containment, eradication, and recovery.

These are just a few examples of cybersecurity testing methods that organizations can use to assess and improve their security posture. There is no one size fit all testing method. Each type of testing serves a specific purpose in identifying and addressing security vulnerabilities and threats. Organizations can adopt the best-fit testing methods or combination of testing methods that is tailored to their specific needs.

6.4 User Information

User Information - Providing comprehensive and user-friendly information to guide users on how to operate the device securely and effectively.

Some recommendations for this documentation should include:

a) User Manual or Instructions for Use (IFU)
Clear and detailed user manuals that outline the proper and secure operation of the medical device. This should include instructions on how to set up and configure security features, possible cybersecurity hazards that the device may pose, as well as best practices for maintaining the security of the device.

b) Security Guidelines
Specific security guidelines and best practices that users should follow to ensure the security of the device and any associated data.

c) Troubleshooting and Support
Information on how to troubleshoot security-related issues and where to seek support if security concerns or incidents arise.

d) Software and Firmware Updates
Guidance on how to apply software and firmware updates to the device to address security vulnerabilities and ensure that the device is running the latest secure versions.

e) Contact Information
Clear contact information for the manufacturer's support team or security response team, so users can easily report security issues or seek assistance.

f) Security Certifications and Compliance
Documentation of any security certifications or compliance standards that the device meets, providing users with assurance of its security measures.

Customer Security Documentation

When it comes to Customer Security Documentation for medical devices, it's essential to provide comprehensive and user-friendly information to guide users on how to operate the device securely. Manufacturers should also effectively communicate relevant security information when operating the medical device in its intended environment. The following elements 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 usage environment.
- A description of the systematic procedures for authorized 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).

Due to the potentially sensitive nature of these information, which may disclose the strengths and weaknesses of a medical device's cybersecurity; it is advisable for the manufacturers to establish a secure communication channel for distributing such information to the users.

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

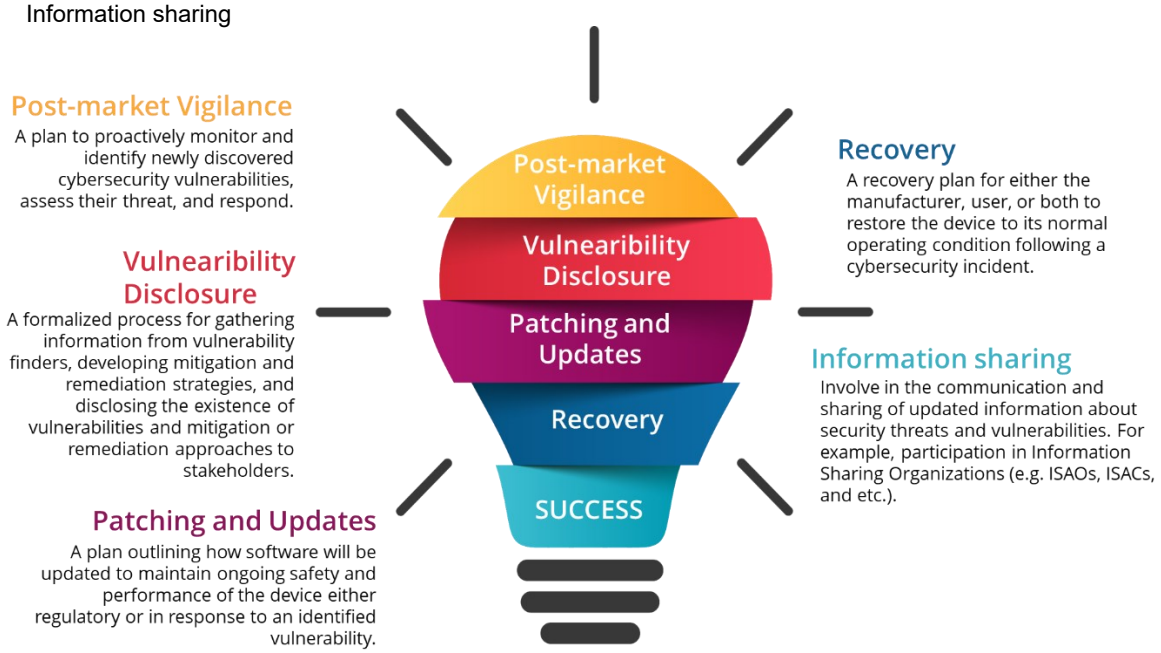

Figure 3: Key considerations for the post-market plan.

By addressing these pre-market elements, manufacturers can enhance the cybersecurity of their medical devices and contribute to the overall safety and reliability of the healthcare technology and services provided.

6.6 Software Bill of Materials (SBOM)

The concept of SBOM was initiated by US National Telecommunications and Information Administration (NTIA) in 2018 to address software transparency. NTIA defined SBOM as a “list of one or more identified components, their relationships, and other associated information.”

In short, SBOM is a comprehensive list of the software components used in building a particular application or system. This includes all the open-source and third-party components, libraries, and dependencies that are utilized in the development of the software.

The adoption of SBOM has become increasingly important, especially in the context of cybersecurity. Leveraging on SBOM allows organizations to track and manage the software components used in their systems, which is essential for identifying and addressing potential vulnerabilities, the “weak link” and security risks in the software supply chain.

In the context of medical devices, having an SBOM is particularly important as it enables manufacturers, users and healthcare providers to understand the software components and potential security implications. It also facilitates the tracking of software updates and patches, aiding in the maintenance of a secure and reliable medical device ecosystem.

While the selection of SBOM formats is out of the scope of this guide, medical device manufacturers should adhere to recognized SBOM formats to ensure interoperability and facilitate data exchange. When generating an SBOM, choosing a machine-readable format is vital for automated processing and analysis. The following are the SBOM elements to be considered:

- Author name - denotes the entity (such as an individual, organization, 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 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 previously version.
- Unique Identifier – identifiers used to recognize a component or function as a look-up key for relevant databases.
- Relationship - explains how an upstream component X is incorporated into software Y.

The following use cases demonstrate on how SBOMs play a crucial role in enabling organizations 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 Ptd Ltd is a manufacturer of advanced medical imaging equipment. They are committed to ensuring the security and integrity of their devices to protect patient data and maintain the reliability of their products.

Use of SBOM:
ABC Medical Devices utilizes 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.

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 utilizes 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:
Armed with 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 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 for regulatory reporting and demonstrating 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.

6.7 Additional consideration - Devices with Artificial Intelligence (AI)

AI is rapidly emerging as a key field in today's world, with its integration into medical devices enhancing workflow, aiding in diagnosis, and predicting risk of diseases. While AI holds the potential to increase work efficiency and reduce costs, it also may pose intentional and unintentional harm. The swift advancement and uptake of AI could make it a prime target for malicious cyber actors. If a medical device is compromised, it can lead to incorrect diagnoses, treatment errors or even life-threatening situations for patients. With the introduction of Generative AI, new threats such as: prompt injections, hallucinations, spreading of misinformation and unintentional data leaks could emerge. Consequently, these new threats that must be addressed alongside with standard cyber threats.

To ensure the deployment of a robust and secure AI system, the following key areas to be considered throughout the AI system development cycle: security in AI model design, security during AI development (including AI supply chain security), security of AI during deployment, and the security of AI during operation and maintenance post-deployment. Device manufacturers and healthcare providers should consider implementing robust data privacy measures, regularly monitor AI outputs for accuracy and ensure transparency in AI-generated content. Additionally, continuous security assessments and updates to cybersecurity protocols are essential to stay ahead of emerging threats.

In addition, AI developers should be responsibly releasing the AI system after subjecting it to thorough security evaluation. All known limitations of the AI system should be clearly communicated to the users. Users should evaluate the pros and cons of the AI system and its' limitations before deploying it for actual use.

7 Post-market stages

This section described the three post-market stages in the TPLC of the medical device, namely the **Support stage**, **Limited Support stage** and **End of Support stage**. At each post-market stage, there is different degree of involvement by the medical device manufacturers and users (including the healthcare providers) in terms of the responsibility and the support given for the device. As the device reaches its End-Of-Life (EOL) and End-Of-Support (EOS), there is a transfer of responsibility from the manufacturer to the user.

7.1 Support stage

At the post-market Support stage, manufacturers should provide comprehensive cybersecurity support to healthcare providers for the devices in use or deployed (e.g. software patches, software and hardware updates, etc.). Users should have access to the information for them to perform their assessment on the cybersecurity of the device.

7.1.1 Procurement and installation

During the procurement and installation phase, manufacturers should provide the following support:

- Provide **Product Security Documentation** [e.g. Software Bill of Material (SBOM), security test reports]: This security documentation helps to provide product security information to the user to aid them in the risk management during the procurement and deployment of the medical devices.

- Provide **Product Life Cycle Documentation** [e.g. key milestones including the cybersecurity EOL and EOS dates (if available)]: This life cycle documentation provides the user the necessary information to manage the security of the device over the course of the device lifecycle.

    - Information to be provided by manufacturers / requested by healthcare providers includes:
        - The device's operating system
        - The version deployed, including the known open software anomalies in each version
        - Identification of software components
        - Ports and services necessary for the device to function appropriately
        - Firewall rules that can be leveraged to isolate the device and maintain function
        - Expected date of service changes
        - The extent of any available maintenance after the changes
        - Anti-malware capabilities and appropriate definitions (what can be scanned)
        - Security scanning capabilities and appropriate scanning definitions (how to scan)
        - Security logging capabilities
        - Device backup and restore procedures
        - Notification method to receive vulnerability notification
        - Administrative accounts and the ability to manage through a privilege access management tool
        - Additional compensating controls (Note: Compensating controls refer to a type of risk control measure that is deployed in lieu of, or in the absence of, risk control measures implemented as part of the device's design.)

    - The schedule of service changes and the extent of any available maintenance (applicable for the third-party component as well) should be clearly communicated.

- **Contractual agreement** between the manufacturers and healthcare providers for the commitment on the period of cybersecurity support to be provided.

7.1.2 When device is in use

While the device is in use, it is important that the communication between manufacturers and healthcare providers are well-maintained. This is to allow for prompt and adequate support in situations when vulnerabilities emerge. Both the manufacturers and healthcare providers should take note of the following:

- Manufacturers should provide **updated Product Security and Product Life Cycle Documentation**. There will be changes to the device throughout its life cycle. As such, it is crucial for manufacturers to update the healthcare providers of the changes so that they are aware of the new risks involved.

- Manufacturers should provide the relevant **Vulnerability and Patching Information.** If there is any vulnerability discovered, manufacturers should keep healthcare providers informed and provide any mitigations that are available. Such communication between the manufacturer and healthcare providers can help to prevent patient harm or device/service disruption.

- **Monitoring of software components** (e.g. operating systems, third-party components) are necessary to maintain performance of the device, ensure adequate support and allow smooth transition to new components

(e.g. due to EOL/EOS of the component, or as a mitigation to reduce the risk of vulnerability, etc.). Such monitoring should be performed by both manufacturers and healthcare providers, e.g. using SBOM, and carry out risk assessment to determine the impact on the cybersecurity of the device. In such situations, the manufacturer informs the healthcare providers when any component reaches its EOL/EOS, or the healthcare providers engages the manufacturer in their planning for any component nearing EOL/EOS.

- It would be beneficial to include and consider the following information to allow for efficient monitoring:
  - Expected EOL/EOS date (if any)
  - SBOM
  - Any software upgrade option
  - Software changes schedule
  - Maintenance schedule
  - Risk analysis documentation (e.g. the available mitigation, any potential new risk, etc.)

- The support from manufacturers may reduce for component(s) until the device's EOS. However, manufacturer should still monitor and inform healthcare providers if there is any change to the risk profile of the device.

- **Post-market surveillance** of the device is necessary after device deployment. The activities include
  a) Continuous monitoring of the device for potential security threats and anomalies. This involves the collection, documentation and review of all complaints received internally (e.g. during verification and validation) or externally (e.g. customer complaints).
  b) Reporting of any adverse events and/or field safety corrective actions to regulatory authority.
  c) Active engagement in risk management of the device. This allows for prompt management of resources, actions, etc. needed to address the identified security issues / risks impacting the device on an ongoing basis.

- **Cybersecurity training** should be provided for healthcare providers to raise awareness about potential threats and best practices. This is to ensure the healthcare providers understand the importance of security measures and to report if they identify any security concern, to allow for the safe and secure usage of the medical device.

- Manufacturers and healthcare providers are recommended to have a **Vulnerability Management system (VMS)** in place to review and assess vulnerabilities (both new and current) to ensure that the impact of the vulnerabilities to the medical device is reduced to the minimum and with proper security measures (e.g. software updates or patches) implemented.

  The principles to establish an effective VMS include:
  a) Apply update by default:
     By applying update by default, it prevents situations where some updates (feature update or security update) are missed and thus make the medical device 'open' to the vulnerabilities.

  b) Identify assets:
     It is helpful to have a list of components used in the medical device with all the relevant information indicated (e.g. the version, the supplier, EOL/EOS dates, etc.). It is similar to SBOM (refer to the section above).

  c) Triage and prioritise update:
     Sometimes, it is necessary to tackle some vulnerabilities over the others. Therefore, it is important to triage and prioritise some updates to be implemented first to reduce the critical risks.

  d) Justification for not implementing an update:
     Management of cybersecurity risks is part of the device's overall risk management structure. If an update is deemed not required, the rationale for not having an update and the risk assessment of the issue should be documented and assessed by all the relevant parties (e.g. senior management).

  e) Verify and regularly review the system:
     Regular review of the system will allow the system to be up-to-date to identify and review any new threats or vulnerabilities, as well as to monitor the current vulnerabilities. This will ensure the security measures are also updated for the medical device.

7.1.3 Transfer of responsibility

The transition from Support stage to Limited Support stage will result in the transfer of responsibility between the manufacturers and healthcare providers. It is shared responsibility from both sides where manufacturers are capable to provide the maximum support for the device at the start of TPLC, but decreasing support as the device moves towards EOL and EOS of the device. As the device gets nearer to its EOL and EOS, healthcare providers has increasing responsibility to ensure the safety and efficacy of the device.

The best time to start the transition process is approximately 2 to 3 years before the EOS. Manufacturers should inform the healthcare providers the expected EOS date, to allow sufficient time for the healthcare providers to evaluate, plan and budget for the retirement and/or replacement of the device. During this transition process, both manufacturers and healthcare providers should work closely together to allow a smooth transition.

Close communication between the manufacturers and healthcare providers will allow each side to understand their own responsibilities as well as the risks for the device. The following listed some considerations that manufacturers and healthcare providers should consider during this transition process:

Table 1: Consideration by manufacturer and healthcare providers during the transition from Support stage to Limited Support stage.

For manufacturers	For healthcare providers

• Provide updated Product Security Documentation.
• Provide information on the configurable security options that may be implemented at EOL/EOS.
  o Software only
  o Partial software and hardware only
  o Complete replacement:
  (i) Replacement options and strategy
  (ii) Available device models and functionality
• Inform user on the configurable security options.
	• Assess own ability to manage the device from a cybersecurity and clinical use perspective.
	• Identify possible support from third-party and additional resources required which may help to manage and support the device.
	• Assess any potential device replacement opportunities.

7.2 Limited Support stage (Between EOL and EOS)

The Limited Support stage is a crucial stage for medical device as it reached the EOL and moving towards the EOS of its life cycle. Both manufacturers and healthcare providers should continue with the close communication from the Support stage. Information related to the product, possible risks, mitigation and device replacement options should be made available.

At this stage, the manufacturers should inform the healthcare providers of the reduction of support to Limited support. It includes the timeline until EOS, the alerts when some parts of the medical device are no longer supported, any available software updates, any recommended compensating controls. Implementation of compensating controls (i.e. alternative risk control measures) at this stage will be necessary as the device with limited support will not have sufficient protective measures (e.g. no more software updates) against the vulnerabilities.

With lesser support from the manufacturer, the healthcare providers would need to consider if they can continue to use the medical device or to purchase a new device.

The healthcare providers should consider the following points before they decide to continue using a medical device near EOS.

- The risk of using the medical device when the security could be impacted with limited support from manufacturers.
- The usability of the medical device, e.g. whether the limited features still remain applicable to the patients, in cases where there are no software updates (in terms of functionality or security).
- The resources to support the medical device, e.g. compensating controls, maintenance costs.
- The impact to the patients if the medical device cannot be used and an alternative is required.

It is possible that the healthcare providers will purchase a new device after all the above considerations. However, the healthcare providers should also think about the potential gap from the EOS of the current device till the availability of the new device. It is therefore recommended to begin this process approximately 2 to 3 years before the EOS (refer to the Transfer of responsibility above).

7.3 End of Support stage (EOS onwards)

At this EOS stage, full responsibilities are transferred to the healthcare providers where they need to manage the device cybersecurity risks without assistance from the manufacturers. The first step for the healthcare providers is always to assess if they have the capability to handle this transferred responsibility. If necessary, the manufacturers may consider a gradual transfer of responsibility to the healthcare providers, to allow the healthcare providers to have sufficient preparation to take over the responsibility.

Similar to the previous stages in post-market phase, the manufacturer should provide all the necessary product security information to healthcare providers and to inform the public on the move of the medical device to EOS stage. This is critical as it will allow the healthcare providers to perform their assessment / management on the

cybersecurity risks associated with the medical device, or for the public to understand the potential risks in continuing the usage of such EOS device. Besides the cybersecurity risks involved, the potential patient risks should be communicated as part of post-market expectations via reactive vulnerability management.

For the healthcare providers, the same considerations in Limited Support stage remain applicable. In the case where the healthcare providers continue to use the medical device past its EOS date, the following is recommended to allow healthcare providers to have proper management over the cybersecurity risks of the medical device.

- Implement strong cybersecurity program (e.g. resources to manage the increasing risk).
- Implement robust inventory management system (including vulnerability database for third-party components).
- Enhance risk measures (e.g. compensating controls such as limiting physical access, removing remote access, firewall, network segregation/isolation).
- Periodically evaluate the availability of alternative medical device and re-assess the decision to use the current device past its EOS.

With proper risk management measures in place, it will help to ensure the security of the medical device after EOS. In addition to the above measures, it is also recommended that the healthcare providers are trained and be informed on the usage of the medical device in a safe and secure manner and on how to spot and identify any unusual device behaviour. This is to mitigate any risk during the usage of the device.

7.4 Summary

The post-market stage of medical device cybersecurity encompasses the entire period after a device has been released to market. It can be divided into three main phases:

1. Support Stage: This is the primary phase of the device's operational life. During this stage, the manufacturer provides active maintenance and regular updates. Key activities include:
    - Continuous monitoring for new vulnerabilities
    - Releasing timely security patches and updates
    - Providing technical support to users
    - Conducting ongoing risk assessments
    - Implementing cybersecurity improvements as needed

2. Limited Support Stage: As the device ages, it may enter a phase of limited support. During this time:
    - The frequency of updates may decrease
    - Support may be more focused on critical security issues
    - The manufacturer may encourage migration to newer, more secure versions
    - Legacy systems may require additional security measures

3. End of Support Stage: This final stage occurs when the manufacturer no longer provides active support for the device. Key considerations include:
    - Clear communication to users about the end of support
    - Guidance on securely decommissioning devices
    - Strategies for managing cybersecurity risks in legacy devices that must remain in use
    - Potential need for compensating controls to protect unsupported devices

Throughout all these stages, effective cybersecurity management requires collaboration between manufacturers, healthcare providers, and cybersecurity experts. The goal is to maintain the security and integrity of medical devices throughout their entire lifecycle, even as support levels change over time.

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

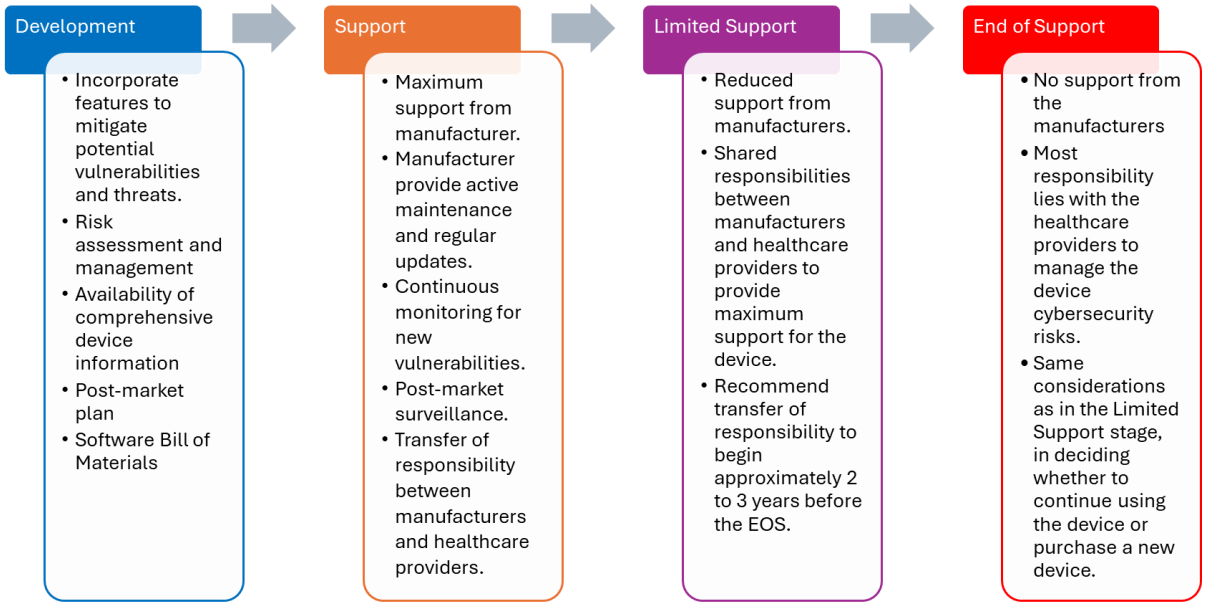

Figure 4: Overview of the cybersecurity best practices in the TPLC of the medical device

8 Conclusion

The landscape of medical device cybersecurity is dynamic and complex, requiring constant vigilance and adaptation from the manufacturers and healthcare providers involved. This document has outlined comprehensive cybersecurity best practices for medical devices, spanning both pre-market and post-market stages of the device's TPLC.

In the pre-market stage, we have emphasised the critical importance of integrating security features from the outset of device development. By incorporating robust risk management strategies, thorough security testing, and transparent documentation including SBOM, manufacturers can lay a strong foundation for device security. These premarket considerations are not merely regulatory checkboxes, but essential steps in creating resilient, secure medical devices that can withstand evolving cyber threats.

The post-market stage, with its support, limited support, and end of support phases, underscores the ongoing nature of cybersecurity in medical devices. As threats evolve and new vulnerabilities emerge, the need for continuous monitoring, timely updates, and proactive risk management becomes paramount. Even as devices approach the end of their supported lifecycle, cybersecurity remains a critical consideration, requiring careful planning and mitigation strategies.

In conclusion, cybersecurity in medical devices requires shared responsibility and close communication between the manufacturers and healthcare providers. By embracing these best practices and fostering a culture of security, we can build a safer, more resilient healthcare ecosystem that leverages the full potential of medical technology while protecting the privacy and safety of patients.

9 Reference

[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