Exploring the Cybersecurity Roles of Manufacturers and Healthcare Organizations During the Medical Device Lifecycle

TLP: WHITE This report may be shared without restriction. For Health-ISAC Members be sure to download the full version of the report from the Health-ISAC Threat Intelligence Portal (HTIP). Contact Membership Services for assistance.

Health-ISAC™
Collaborating for Resilience in Healthcare

health-isac.org

Key Judgements

- Medical devices go through four lifecycle phases, with varying levels of responsibilities placed on the medical device manufacturer and the healthcare delivery organization.
- Healthcare Delivery Organizations should perform more regular risk assessments going into End of Life and End of Support to determine if they can accept the risk of continued use.
- The manufacturer implements Security Control Categories in the development phase to ensure that the device is Secure by Design, Secure by Default, and Secure by Demand.
- Documentation and Transparency are critical in maintaining cybersecurity. This includes providing detailed security documentation, a Software Bill of Materials (SBOM), and clear communication about vulnerabilities and updates.

Introduction

As medical devices become more interconnected and have internet and wireless communications capabilities, understanding the lifecycle stages and the tasks needed to maintain their security posture will help organizations secure devices against cybersecurity threats. The device lifecycle is the various stages a device will go through, from research and development, on the market, and eventually, end of life and end of support. As medical devices move through the lifecycle phases, the responsibility for tasks may transfer between the manufacturers and the customer. Communication between the two parties is essential as the device moves through the lifecycle so that tasks are coordinated, and security gaps within the product are reduced.

This document explores the tasks needed to maintain the cyber resilience of medical devices and how the responsibilities may shift from party to party throughout the total product. The responsibility for maintaining a medical device's cybersecurity posture evolves throughout the lifecycle of a device. The process begins with the device manufacturer during the design and development phase and may increasingly shift to the Healthcare Delivery Organization (HDO) once in clinical use. The International Medical Device Regulators Forum (IMDRF) Principles and Practices for the Cybersecurity of Legacy Medical Devices outlines four lifecycle phases. The Food and Drug Administration (FDA) provides requirements for the cybersecurity of medical devices in the pre-and post-market guidance. Manufacturers can address a device's cybersecurity during design and development using the premarket requirements. Post-market requirements are needed due to cybersecurity risks continuing to evolve after the medical device reaches the market.

Device Lifecycle Phases

The IMDRF recognizes four medical device lifecycle phases: development, support, limited support, and end of support. The development phase of a device is where research and development occur, and documentation is submitted to chronicle the cybersecurity posture, support the regulatory review process, and ultimately bring the product to market. In the support phase, the device is on the market and will typically receive regular updates to improve clinical functionality and user experience, as well as patches to maintain an adequate security posture. In the limited support phase, the HDO continues to use the device for patient care, even though the manufacturer is no longer selling the device on the market. The device may still receive updates and patches; however, the healthcare organization will take on more responsibility for monitoring and accepting the risks associated with continued use of the medical device. Last is the end of the support phase, where the Medical Device Manufacturer (MDM) no longer provides updates or patches, but the HDO has determined to keep the device operational. Proper management of a medical device's lifecycle ensures patient safety and the ability of a device to remain reasonably secure by reducing and managing risks.

Figure 1: IMDRF Lifecycle Chart.

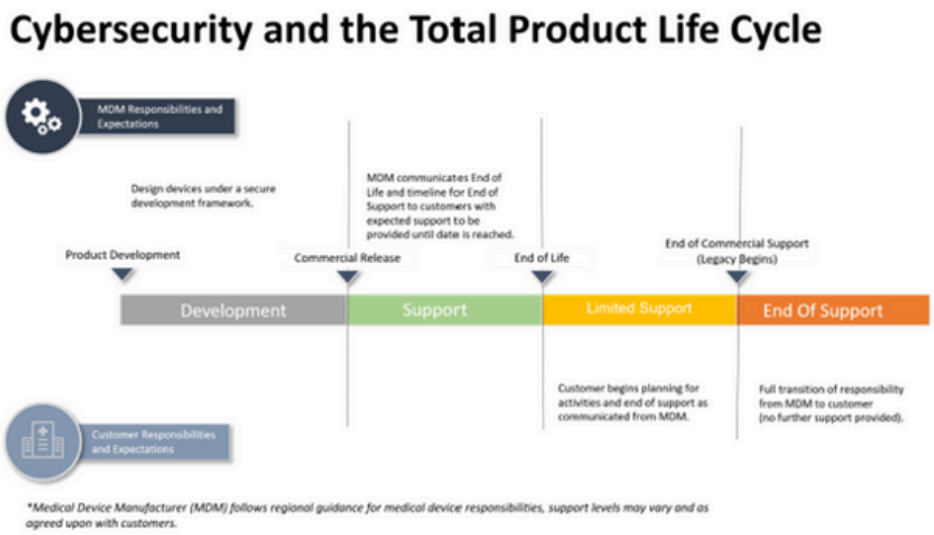


Figure 1: High-level legacy device conceptual framework as a function of product life cycle for cybersecurity

In the development phase, cybersecurity starts with researching, prototyping, reviewing, and testing the new device before making it publicly available.[1] The development phase is also known as the premarket stage. HDO input may inform some features and requirements before and during the development phase by giving feedback on the device's clinical and cybersecurity needs. When creating a device, MDMs should consider the principles of safe by design, safe for users, secure by design, secure by default, and secure by demand. This guidance encourages manufacturers to consider what baseline security controls are needed for the device, patients, and users' security and safety. During the development phase, a manufacturer must assess threats, select components, design security controls, and create documentation on the security posture of the device and its components. Responsibility for cybersecurity features mainly falls onto the MDMs in the development phase of a device. When an MDM is ready, it will submit documentation to the FDA to demonstrate that the device meets proper standards for patient safety, data protection, device reliability, and regulatory compliance. What documentation is needed will depend on the type of device and the regulatory pathway selected to bring it to market. *Appendix IV of the FDA's Premarket Guidance: Cybersecurity Risk Management Report, Measures and Metrics, Architecture Views, Testing, Labeling, and Cybersecurity Management Plans* outlines examples of recommended documentation. The Cybersecurity and Infrastructure Security Agency (CISA) has introduced three product security concepts. *Secure by Design* sets the expectation that manufacturers produce secure products. *Secure by Default* sets the expectation that manufacturers deliver products with secure configurations out-of-the-box. Secure by Demand sets the expectation that customers demand adequately secure devices and services to maintain the cyber posture of the products they procure. Well-established communication channels between HDOs and MDMs are essential for creating a collaborative and cooperative approach to producing and operating cybersecure technologies.

After launching a new medical device, the support phase begins, where devices are approved for sale and used in patient care. Section 7.1.1. of the IMDRF Cybersecurity Management for Legacy Devices lists necessary documentation, including MDS2, Software Bill of Materials (SBOM), security test reports, customer security documentation, and product lifecycle documentation. These documents help HDOs understand risks and develop cyber support strategies.

Manufacturers and HDOs must negotiate roles and responsibilities to maintain device cyber resilience. FDA post-market guidance is relevant, requiring tracking systems, incident reporting, and device registration.

Documentation should be provided to aid in transferring risk between MDMs and HDOs. MDMs should identify tasks and timelines for secure device support, including configuration instructions, patch/update instructions, specific controls (e.g., firewalls, network isolation, VPNs), SBOMs, and MDS2. HDOs should assess technology risks and plan to manage them, either independently or with MDM/third-party aid. These risk assessments aid in understanding and negotiating cyber maintenance responsibilities as the device progresses through its lifecycle.

As a product progresses, the MDM should document key lifecycle milestones, recall details, and software components for the HDO. During responsibility transfer, the manufacturer should inform the healthcare organization about EOL and EOS devices, residual risks, control techniques, monitoring recommendations, and upgrade or replacement options.

Manufacturers must monitor for emerging vulnerabilities, assess their exploitability and clinical impact, and prioritize remediation based on risk. They develop mitigation strategies that consider the HDO environment. If a risk is uncontrolled, manufacturers will provide mitigations through patches or updates.

The third phase is limited support, where devices are still used for patient care but are no longer marketed or sold and have been declared end-of-life by the manufacturer. Communication between MDMs and HDOs increases to ensure HDOs understand the risks of using devices past active support. MDMs should provide lifecycle planning, security documentation, and customer notifications, including end-of-support dates. The IMDRF recommends two to three years of advance notice for end-of-life and end-of-support notifications to allow customers to assess the risks and determine strategies for replacement or continued operations.

HDOs should perform annual or more frequent risk assessments to determine essential cyber maintenance tasks and evaluate risks of purchasing, continued use, or repurposing devices near EOS. Regular security assessments help HDOs understand and manage cyber risks, improving resilience and posture.

The End of Support (EOS) phase begins when the MDM announces it will no longer update or service the device. The HDO may opt to keep EOS medical devices operational due to cost, necessity, lack of alternatives, and operational constraints. The MDM provides security information, including the upgrade path and decommissioning details. Responsibility remains with the MDM to monitor for severe cyber risks and respond if necessary. The FDA's post-market guidance does not explicitly require this. Figure 2: A detailed legacy device framework as a function of the product life cycle for cybersecurity, found on page 34 of the IMDRF Principles and Practices for the Cybersecurity of Legacy Medical Devices guidelines, which suggests that it remains in effect.

During EOS, the HDO assumes almost all responsibility and may adjust contract terms based on support needs. The HDO should conduct a risk assessment to determine the maximum acceptable risk level. Device users should consider decommissioning devices with unsupported components due to cybersecurity threats. The HDO may keep the device operational due to cost, necessity, lack of alternatives, and operational constraints.

Secure Control Categories

FDA outlines security controls to be considered for medical devices in Appendix 1, Security Control Categories and Associated Recommendations of the FDA Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, issued on September 27, 2023.

Several security control categories are recommended for a device to ensure its security and the user's and patient's safety. These include authentication, authorization, integrity, cryptography, confidentiality, event detection and logging, resiliency and recovery, firmware, and software updates. Confidentiality, Integrity, and Availability, often called the CIA triad, are the three pillars of developing a security system.

Authentication in a secured system involves entities and information. Entity authentication verifies the identity of endpoints (hardware or software). Information authenticity ensures data comes from a trusted source and remains unaltered during transit. A robust system can authenticate stored and transmitted information, communication endpoints, and running software integrity.

MDMs can use implicit or cryptographic authentication schemes. Implicit schemes may allow unauthorized access by mimicking authorized behavior. Cryptographic schemes, which encode and decode messages, are more robust.

Once a user or entity is authenticated to the device or system, **authorization** controls what resources that user has permission to access, such as applications, data, files, or objects. An effective authorization scheme enforces zero trust principles like least privilege and reauthentication for every transaction to ensure proper permissions are maintained throughout the session. This prevents lower-privilege users from accessing sensitive resources. MDMs and HDOs can limit access using passwords, certificates, and biometrics.

Cryptography: Cryptographic algorithms and protocols protect data at rest and in transit, supporting FDA security by design objectives. Manufacturers should use industry-standard cryptographic methods and avoid deprecated algorithms, following National Institute of Standards and Technology (NIST) standards like SP 800-131A Transitioning the Use of Cryptographic Algorithms and Key Lengths.

Security architecture should prevent a single device compromise from revealing keys for others, limiting breach impact. Cryptographic protocols like TLS and SSL, using RSA algorithms and certificates, secure data exchange through Public Key Infrastructure.

The principle of **integrity** applies to code, data, and execution. Code integrity ensures that the software, firmware, and configurations are not tampered with before execution by protecting the code from malicious code, bugs, or unauthorized changes. Methods to defend code integrity include:

- Hardware-based security solutions.
- Verifying authentication tags.
- Allowing installation of cryptographically authenticated updates.
- Disabling or restricting unauthorized access.
- Employing tamper-evident seals on devices and their communication ports.

Data integrity verifies that an unauthorized process or entity has not altered the data elements. Recommendations for this include:

- Verifying the accuracy and trustworthiness of all incoming data.
- Ensuring the data from external sources are well-formed and compliant with protocol specifications.

Execution integrity verifies that code remains secure and runs correctly during runtime rather than only verifying the code before execution. Runtime attacks may include memory corruption or code injection as a means of altering the executable after it is loaded. Ensuring execution integrity includes utilizing industry best practices such as digital signatures, checksums, and secure boot processes to maintain and verify code integrity after carefully designing and reviewing all code.

Confidentiality is crucial for all parties to prevent patient harm from data breaches. Breaches can occur through unauthorized credential use, exposed information, or device misuse. Ensuring confidentiality involves robust authentication and authorization. Cybersecurity teams must integrate these tools during threat modeling and risk management.

Compromised medical devices can reveal extensive data. IoT devices linked to electronic health records (EHR) capture patient identifiers, demographics, diagnoses, medications, procedures, lab results, vital signs, and utilization events. Beyond EHR, breaches can expose organizational, administrative, behavioral, sentiment, and pharmaceutical data. Effective cybersecurity measures are essential to protect this diverse information.

Event detection and logging are essential for identifying and tracking attempts to compromise medical devices and maintaining visibility. Cybersecurity teams in HDOs use these tools to detect changes, such as unauthorized access or devices going offline. Users and stakeholders should be notified of malfunctions or malicious behavior.

Medical device manufacturers (MDMs) should implement features to detect, log, time, and respond to compromises during regular use. Devices need storage for forensic discovery and tracking capabilities. An Intrusion Detection System (IDS) captures forensic evidence, and documentation should detail log file management.

MDMs should conduct variant analyses to identify vulnerabilities in device models and product lines. Security configurations must address gaps and limit vulnerabilities. Devices should generate an SBOM in a machine-readable format, listing components for vulnerability management. MDMS are encouraged to share SBOMs to the public but, there is no current documentation requiring this. Depending on their components, devices can integrate antivirus/anti-malware protection. Software configuration management tools should be available to authorized users to track and control software changes.

Resiliency and Recovery: A device's cyber resiliency ensures it remains available and functional during cyber incidents, providing a safety margin against unknown vulnerabilities. To achieve this, critical functionality and data protection features should be implemented. MDMs can design devices to preserve data, logs, and system information for specific periods, including data copies. Devices should withstand cybersecurity incidents like network outages, DDoS attacks, and port scanning. They must also recover systems or data affected by incidents. A cyber-resilient device maintains integrity and confidentiality during such events.

Firmware and Software Updates: Updating and patching a device enhances security and fixes vulnerabilities. Updates improve functionality, efficiency, security, or user experience, while patches address discovered vulnerabilities and can be part of updates. Device owners should be informed of any changes. Manufacturers should design devices for easy updating, rapid testing, evaluation, and patching in the field. Tools for developing and testing the original device should be maintained for creating updates and patches. The update process must be reliable, even during communication breaks, and anticipate future software and firmware needs.

Contingency plans are necessary if a third party stops supporting a licensed product. Healthcare facilities must consider diverse patch needs and lag times to minimize operational disruptions. Effective communication, standardization, and documentation between manufacturers and HDOs ensure updates and patches are applied with minimal downtime, protecting against vulnerabilities and meeting regulatory standards.

Monitoring and response are integral to risk management. Organizations should surveil systems for vulnerabilities or suspicious activities and respond with mitigation strategies, patching, or updates. Indicators of compromise (IOCs) help detect system infiltrations, enabling cybersecurity teams to implement remediation.

MDMs can provide HDOs with documentation for monitoring and forensic analysis, including logs, SBOMs, secure configuration recommendations, and threat models. Once installed, MDMs may continue monitoring devices through machine monitoring, IoT remote monitoring, access controls, and key performance indicators (KPIs). Network monitoring tools detect issues or suspicious activity, while HDOs can integrate devices into their network security infrastructure to protect sensitive data.

Tasks and Responsibilities

To maintain the cyber resilience of medical technology, successful collaboration between MDMs and HDOs is essential. Both parties must address various cybersecurity tasks throughout the device lifecycle. The FDA mandates monitoring and response plans for emerging threats and vulnerabilities but does not specify the exact tasks. Key tasks include communication, transparency, risk assessment, risk management, documentation, patching, updating, security controls, monitoring, and response.

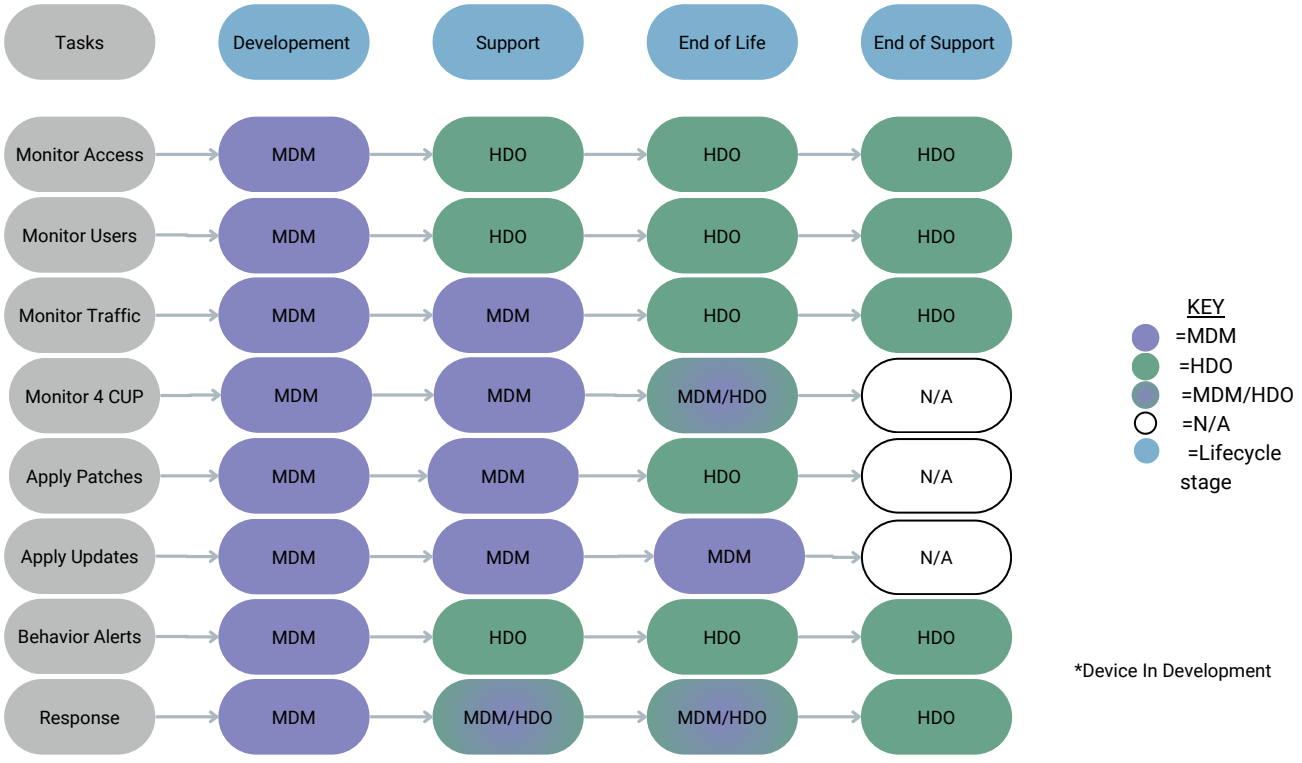
Clear identification and **communication** of responsibilities are crucial to avoid a diminishing security posture over the device's life. Responsibilities may shift from the MDM to the HDO as the device progresses through its lifecycle. HDOs must identify which tasks they can support and ensure remaining tasks are assigned to alternate providers. MDMs typically cease providing technical support, including updates and patches, at the end of the service lifecycle.

Transparency and **documentation** are vital for securely implementing a medical device. This includes sharing information on configuring or updating the device and other relevant details to promote safe and effective use. Critical details, such as communication interfaces and third-party software, must be communicated to highlight potential risks. Vulnerability disclosures are necessary to reestablish system resiliency. Sharing customer-facing versions of artifacts from FDA premarket guidance can demonstrate a device's security posture.
Effective communication between MDMs and HDOs is essential for device security and safety. During development, MDMs and HDOs establish communication strategies, with MDMs receiving feedback on required documentation and device needs. MDMs provide tools like threat assessments, risk assessments, baseline controls, secure configuration settings, and update schedules. Ongoing communication includes notifying any device component changes and involving third parties to alert known security risks.

Risk management involves navigating potential threats posed by medical devices within the healthcare organization. This ongoing process starts with the MDM during development and transitions to the HDO during operation. MDMs provide documentation on baseline security controls and risk analysis. Methods to examine potential risks include threat modeling, risk assessments, interoperability considerations, third-party software components, and vulnerability assessments. Threat modeling identifies risks and develops mitigations, while risk assessments determine the severity of cybersecurity failures. Interoperability considers communication boundaries and protocols, and vulnerability assessments evaluate the need for responses to flaws impacting patient safety, data privacy, or device availability.

Lifecycle Changes

Figure 2: Sample of Cyber Resilience Task Distribution over the Lifecycle



As a device progresses through its lifecycle, several tasks transition from the MDM to the HDO. These tasks include monitoring access, users, and traffic, applying updates and patches, and responding to behavior alerts.

During the development phase, the MDM configures the device to address safety issues and risks, implementing monitoring capabilities for access, users, and traffic. Once in support, the HDO takes over monitoring access and users, while the MDM may continue monitoring traffic until the end-of-life (EOL) phase.

Updating and patching begin in the development phase, where the MDM identifies vulnerabilities, applies patches, and tests mitigations. The MDM also plans post-market monitoring and patch programs. In the support phase, the MDM continues to monitor and mitigate vulnerabilities. During limited support, not all software components may receive updates. At EOL, the HDO assumes responsibility for cyber maintenance, assessing risks of continued device use.

MDMs should implement event detection and logging features during development. In the support phase, the HDO logs and monitors events for unexpected behaviors, indicating unauthorized access or vulnerabilities.

Security event monitoring and response start in development, with the MDM conducting security testing and risk mitigation. In support, the MDM may handle backup, recovery, and event tracking while the HDO manages IT security monitoring and patching. The MDM continues to monitor the external environment, perform security testing, and address discovered risks. The HDO should ensure devices are securely integrated into the network and monitor network traffic for evidence of intrusion and exploitation.

Conclusion

Maintaining medical device security, reliability, and safety throughout its lifecycle is crucial for patient safety and regulatory compliance. MDMs and HDOs have distinct responsibilities that shift as devices progress through their lifecycle stages. Effective collaboration and adherence to safety guidelines strengthen device security within the healthcare system.

MDMs should implement security tools during the development phase to ensure device security. Continuous communication between MDMs and HDOs is essential for mitigating risks. Event detection and logging provide forensic evidence if a device is compromised. Updating and patching require collaboration to address vulnerabilities and enhance device resilience. By clearly defining and agreeing on responsibilities at each lifecycle stage, MDMs and HDOs can effectively maintain medical device security and resilience.