# Medical Device Product Cybersecurity Guide

## Table of Contents

# Section 1: Introduction to Medical Device Product Security

## What is Medical Device Product Security?

Medical device product security refers to the discipline of designing, developing, deploying, and maintaining medical devices in a way that ensures confidentiality, integrity, and availability (CIA) of device data and functionality across the product lifecycle.

This includes implementing technical controls, risk management, and compliance measures to mitigate threats that could compromise patient safety or regulatory compliance.

*Source: FDA Postmarket Management of Cybersecurity in Medical Devices, 2016*

## Why Is It Critical?

- **Patient Safety:** Exploited vulnerabilities in connected devices can directly affect diagnosis or treatment (e.g., incorrect insulin delivery or pacemaker signal manipulation).
  *Source: FDA Cybersecurity Guidance for Premarket Submissions, 2023*
- **Regulatory Requirements:** Manufacturers must comply with cybersecurity expectations defined by the FDA, ISO 14971, IEC 62304, and other global frameworks.
- **Reputation & Liability:** Breaches in product security can lead to recalls, regulatory penalties, and loss of trust.
  *Source: St. Jude Medical Recall – FDA Safety Communication*

## What Is a Secure Medical Device?

A secure medical device is one that:

- Has undergone cybersecurity risk assessment as part of product design (per ISO 14971)
- Follows a secure software development lifecycle (per IEC 62304)
- Implements technical security controls such as authentication, encryption, and secure boot
- Is monitored postmarket for vulnerabilities and can be updated or patched securely

*Sources: NIST Cybersecurity Framework (NIST CSF), FDA Premarket Cybersecurity Guidance, 2023*

## Who Is Responsible?

Product security is a cross-functional responsibility involving:

- R&D and Software Engineers – for secure design and implementation
- Quality & Regulatory Teams – for compliance with FDA, 21 CFR Part 820, and IEC standards
- Security & IT – for architecture reviews, monitoring, and incident response
- Clinical and Risk Teams – for evaluating potential patient harm

*Source: 21 CFR Part 820 – FDA Quality System Regulation*

## Common Cyber Threats to Medical Devices

Medical devices are often targeted due to their clinical importance and connectivity. Common threats include:

- Unauthorized access to device functions
- Data exfiltration or tampering (e.g., ePHI)
- Exploitation of unpatched software components
- Ransomware affecting hospital networks and IoMT devices

*Sources: HSCC Medical Device and Health IT Joint Security Plan, 2019, FDA Safety Communication: Cybersecurity Vulnerabilities in Insulin Pumps*

## Medical Device Lifecycle & Security Integration

Security must be embedded across the entire lifecycle of a medical device:

| Stage | Security Focus | Standards/Regulations |
|---|---|---|
| **Concept & Design** | Threat modeling, requirements definition | FDA Premarket Guidance, ISO 14971 |
| **Development** | Secure coding, vulnerability testing | IEC 62304, OWASP, FDA Premarket Guidance |
| **Verification** | Security validation & risk mitigation documentation | ISO 14971, 21 CFR Part 820 |
| **Market Release** | Cybersecurity documentation in 510(k) or PMA submission | FDA Submission Guidance |
| **Postmarket** | Monitoring, patching, coordinated disclosure | FDA Postmarket Guidance, ISO 30111 |

# Section 2: Regulatory Frameworks

## 2.1 FDA Cybersecurity Guidance

The U.S. Food and Drug Administration (FDA) requires that manufacturers address cybersecurity across the entire lifecycle of medical devices. The FDA does not mandate specific controls but expects manufacturers to adopt a risk-based approach using recognized standards such as ISO 14971, IEC 62304, and NIST CSF.

There are two key guidance documents:

**FDA Premarket Cybersecurity Guidance**

*"Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" (FDA, Final Guidance, September 2023)*

**FDA Postmarket Cybersecurity Guidance**

*"Postmarket Management of Cybersecurity in Medical Devices" (FDA, Final Guidance, December 2016)*

### Premarket Cybersecurity Expectations

For all submissions including 510(k), PMA, and De Novo, the FDA expects the following cybersecurity documentation to be included:

- **Threat Modeling and Risk Analysis**
  - Identify potential cybersecurity risks that could affect device functionality or patient safety
  - Align with ISO 14971 and threat modeling frameworks such as STRIDE
- **Security Requirements**
  - Documented cybersecurity design inputs based on risk analysis
- **Design Controls and Architecture**
  - Description of secure design features, including authentication, encryption, secure boot, and update mechanisms
  - Aligned with 21 CFR Part 820 – Design Controls
- **Software Bill of Materials (SBOM)**
  - Inventory of all software components, including third-party libraries and their known vulnerabilities (CVEs)
  - Supports vulnerability management postmarket
- **Security Testing and Verification**
  - Include results from static/dynamic analysis, fuzz testing, penetration testing, and validation of implemented controls

- Mapped to software lifecycle processes in IEC 62304

➢ **Labeling and User Documentation**

- Cybersecurity-related instructions for users, such as password policies, update procedures, and limitations

➢ **Plan for Ongoing Security Management**

- Postmarket strategy for vulnerability disclosure, patching, and updates
- Reference to FDA Postmarket Guidance and frameworks like NIST 800-53 or ISO 27001

### Postmarket Cybersecurity Expectations

Once a device is on the market, manufacturers are expected to:

➢ **Monitor for New Vulnerabilities**

- Leverage threat intelligence sources (e.g., NVD, ICS-CERT)
- Evaluate how new vulnerabilities affect device safety and effectiveness

➢ **Perform Risk Re-Evaluation**

- Assess whether new threats create unacceptable risks under ISO 14971

➢ **Communicate and Disclose**

- Follow a Coordinated Vulnerability Disclosure (CVD) process in line with ISO 30111 and ISO 291479
- Report issues to FDA when necessary (e.g., through Medical Device Reporting [MDR] or Recalls)

➢ **Deploy Security Updates**

- Timely remediation through validated patches
- Ensure updates are delivered securely and do not compromise device functionality

## 2.2 ISO 14971 – Medical Device Risk Management

ISO 14971 is the internationally recognized standard for risk management of medical devices, including those with software and cybersecurity components. It provides a structured approach for identifying, evaluating, controlling, and monitoring risks associated with medical devices throughout their lifecycle.

*Standard Reference: ISO 14971:2019 – Application of Risk Management to Medical Devices*

### Purpose in Cybersecurity:

While ISO 14971 was originally focused on patient safety, the FDA and global regulators expect manufacturers to include cybersecurity risks in their risk management process. Cyber threats that could impact device functionality, patient harm, or data integrity must be assessed alongside traditional hazards.

*Referenced in:*

- **FDA Premarket Cybersecurity Guidance, 2023**
- **FDA Postmarket Cybersecurity Guidance, 2016**
- **IMDRF Cybersecurity Principles and Practices, 2020**

### Key Cybersecurity Applications of ISO 14971:

- **Hazard Identification**
  - Include cybersecurity-related hazards (e.g., unauthorized access, malware, unpatched software) that could affect safety or effectiveness.
- **Risk Analysis**
  - Analyze cyber threats using structured threat modeling (e.g., STRIDE, MITRE ATT&CK).
  - Consider both likelihood of exploitation and severity of harm to the patient.
- **Risk Evaluation**
  - Determine if the risk is acceptable based on predefined acceptance criteria.
- **Risk Control Measures**
  - Define and implement technical (e.g., encryption, authentication) and procedural (e.g., user training, patching) mitigations.
  - Verify effectiveness of controls.
- **Residual Risk Assessment**
  - Evaluate risks that remain after controls are applied — if still unacceptable, apply additional layers of protection.
- **Risk-Benefit Analysis**
  - If residual risk cannot be fully mitigated, justify it based on the device's clinical benefit.
- **Postmarket Monitoring**
  - Reassess risks as new threats, CVEs, or incidents arise (aligned with FDA postmarket expectations).

## 2.3 IEC 62304 – Medical Device Software Lifecycle Processes

IEC 62304 is the international standard that defines the software development lifecycle (SDLC) for medical device software. It provides a structured framework for safe design, development, maintenance, and risk management of software — including embedded code, standalone apps, and firmware in medical devices.

*Standard Reference: IEC 62304:2006 + A1:2015 – Medical Device Software – Software Life Cycle Processes*

## Purpose in Cybersecurity:

IEC 62304 doesn't explicitly focus on cybersecurity, but FDA, IMDRF, and MDCG (EU) recognize it as essential for integrating secure software development practices into the lifecycle of a medical device.

*Referenced in:*

- FDA Premarket Cybersecurity Guidance, 2023
- IMDRF Cybersecurity Guidance, 2020
- MDCG 2019-16 – Guidance on Cybersecurity for Medical Devices (EU)

## Key Cybersecurity Applications of IEC 62304:

- **Software Safety Classification (A, B, C)**
  - Devices are categorized based on potential harm to the patient if the software fails.
  - Cybersecurity threats that could lead to software failure or unsafe conditions must be considered in the classification.
- **Secure Design Inputs & Architecture**
  - Document security requirements early in design (e.g., encryption, access control, authentication).
  - Include threat modeling as part of software architecture reviews.
- **Secure Coding Practices**
  - Adopt industry coding standards (e.g., OWASP, CERT C/C++) to prevent common vulnerabilities such as buffer overflows or injection flaws.
  - Enforce code reviews and static analysis.
- **Software Verification & Validation (V&V)**
  - Perform unit testing, integration testing, system testing, and security testing (e.g., fuzzing, SAST, DAST).
  - Ensure implemented security features function as intended.
- **Configuration & Change Management**
  - Document and control software versions, patches, and updates.
  - Align with FDA expectations for postmarket patching procedures.
- **Software Maintenance Planning**
  - Include a plan for addressing discovered vulnerabilities, issuing updates, and tracking bug fixes across software versions.

# 2.4 IEC 62443 – Industrial and Embedded Device Cybersecurity

IEC 62443 is a series of international standards developed by ISA and IEC that focus on cybersecurity for industrial automation and control systems (IACS) including embedded medical systems. While originally intended for industrial environments, it has become increasingly relevant for network-connected and embedded medical devices.

*Standard Reference: IEC 62443 – Security for Industrial Automation and Control Systems*

## Why It Matters for Medical Devices:

Many medical devices now function as cyber-physical systems — often embedded, network-connected, or part of hospital infrastructure (e.g., infusion pumps, imaging systems, surgical robots). IEC 62443 helps manufacturers apply secure design principles to these systems.

*Referenced in:*

- FDA Premarket Cybersecurity Guidance, 2023
- IMDRF Cybersecurity Guidance, 2020
- MDCG 2019-16 – EU Cybersecurity for Medical Devices

## Relevant Parts of IEC 62443 for Product Security

IEC 62443 is divided into four major categories:

| Part | Focus Area | Relevance to Medical Devices |
|---|---|---|
| **62443-1-x** | General concepts | Terminology, definitions, metrics |
| **62443-2-x** | Policies & procedures | Security programs, patching, updates |
| **62443-3-x** | System-level security | Security architecture & zones/conduits |
| **62443-4-x** | Component-level security | Embedded device security requirements |

## Key Cybersecurity Applications for Medical Devices:

- **Secure System Architecture (Zones & Conduits)**
  - Apply **segmentation and trust boundaries** between device functions, networked components, and external interfaces.
  - Supports **defense-in-depth** and **least privilege** design principles.
- **Embedded Device Requirements (62443-4-2)**
  - Define technical security features for medical devices, such as:
    - Authentication mechanisms
    - Secure communications (TLS, IPsec)
    - Security logging
    - Secure firmware updates
    - Account & credential management
- **Security Development Lifecycle (SDL)**
  - Aligns closely with IEC 62304 and includes:
    - Threat modeling
    - Secure design reviews
    - Vulnerability testing

- Risk-based patching strategy

➢ **Vendor and Supply Chain Security**
- Encourages secure procurement and third-party component validation, a critical need in SBOM-driven compliance (e.g., FDA and EO 14028).

## 2.5 ISO/IEC 27001 – Information Security Management Systems (ISMS)

ISO/IEC 27001 is the international standard for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). It applies to organizations that handle sensitive data, including those managing medical device data, software platforms, cloud services, and connected health systems.

*Standard Reference: ISO/IEC 27001:2022 – Information Security, Cybersecurity, and Privacy Protection – ISMS Requirements*

### Why It Matters for Medical Device Cybersecurity:

While ISO 27001 is not specific to medical devices, it's highly relevant for:

- Manufacturers offering connected medical devices or cloud-based platforms
- Organizations managing ePHI, telemetry, or patient data from devices
- Aligning postmarket monitoring, incident response, and breach notification policies with regulatory expectations

*Referenced in:*

- FDA Postmarket Cybersecurity Guidance
- HIPAA Security Rule (U.S.)
- EU GDPR Security Requirements
- IMDRF Cybersecurity Guidance (2020)

### Key Cybersecurity Applications of ISO/IEC 27001:

➢ **Risk-Based Security Program**
- Requires organizations to identify security risks and apply risk treatments using controls from ISO/IEC 27002.
- Supports cyber risk management for product ecosystems, including device-to-cloud communications.

➢ **Security Policies & Governance**
- Formalizes internal cybersecurity policies, user access controls, password policies, and audit procedures.
- Encourages integration with product security teams and quality systems.

➢ **Access Control & Identity Management**

- Ensures strong access controls to sensitive systems (e.g., configuration tools, code repositories, or device cloud platforms).
- Maps well to device access requirements in IEC 62443-4-2 and FDA guidance.

➢ **Incident Response & Business Continuity**

- Requires documented incident response plans, logging practices, backup procedures, and disaster recovery testing.
- Aligns with FDA postmarket requirements for incident handling and HIPAA breach notification.

➢ **Third-Party & Supply Chain Risk Management**

- Evaluates security posture of vendors, suppliers, and partners involved in the device development lifecycle.
- Critical for managing risks associated with open-source components and SBOMs.

## 2.6 NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework (CSF) is a flexible, risk-based approach to managing cybersecurity across critical infrastructure sectors, including healthcare and medical devices. It was developed by the National Institute of Standards and Technology (NIST) and is widely used by regulators, manufacturers, and healthcare providers.

*Standard Reference: NIST Cybersecurity Framework v1.1 (2018)*

*Update: NIST CSF 2.0 was released in February 2024, introducing a new "Govern" function and reinforcing the importance of supply chain, SBOM, and continuous improvement.*

### Why It Matters for Medical Device Cybersecurity:

Although not a regulatory requirement, NIST CSF is referenced in FDA Postmarket Cybersecurity Guidance and provides a proven structure for building secure medical device ecosystems. It supports manufacturers in:

- Aligning organizational cybersecurity with product-level controls
- Developing postmarket monitoring and response plans
- Supporting ISO 27001 alignment and risk-based approaches
- Enhancing internal cybersecurity maturity models

*Referenced in:*

- FDA Postmarket Cybersecurity Guidance (2016)
- IMDRF Cybersecurity Guidance (2020)
- Healthcare & Public Health Sector Coordinating Council (HSCC) Joint Security Plan (2019)

### The Five Core Functions of NIST CSF (v1.1 & v2.0):

| Function | Purpose | Examples in Medical Devices |
|---|---|---|
| **Identify** | Understand risks and assets | Maintain SBOM, classify data flows, map threat models |

| | | |
|---|---|---|
| **Protect** | Implement safeguards | Apply access controls, encryption, segmentation |
| **Detect** | Monitor systems for anomalies | SIEM alerts, endpoint telemetry, anomaly detection |
| **Respond** | Contain and mitigate threats | Incident response plans, containment workflows |
| **Recover** | Restore services and update controls | Firmware rollback, restore backups, root cause analysis |

*Note:* CSF 2.0 adds a 6th function: Govern — focused on strategy, roles, and oversight of cybersecurity programs.

## 2.7 21 CFR Part 820 – FDA Quality System Regulation (QSR)

21 CFR Part 820 is the U.S. FDA's Quality System Regulation (QSR), which outlines requirements for design, manufacturing, process control, and postmarket surveillance of medical devices. While it does not explicitly mention cybersecurity, it applies to all aspects of product safety and effectiveness, which includes security risks that could affect device function or patient health.

*Regulation Reference: 21 CFR Part 820 – Quality System Regulation*

### Why It Matters for Cybersecurity:

The FDA expects cybersecurity risks to be managed as part of overall product quality, especially under Design Controls (820.30) and Corrective and Preventive Actions (CAPA – 820.100). Security vulnerabilities are treated like any other defect that could affect safety or effectiveness.

*Referenced in:*

- FDA Premarket Cybersecurity Guidance (2023)
- FDA Postmarket Cybersecurity Guidance (2016)
- FDA Guidance on Applying Human Factors to Medical Devices (for user access/security features)

### Key Sections of 21 CFR Part 820 That Apply to Cybersecurity:

- **820.30 – Design Controls**
  - Requires security requirements to be included during the design phase
  - Cybersecurity risk analysis (e.g., via ISO 14971) must be documented
  - Security functions (e.g., access control, secure update mechanisms) must be verified and validated
- **820.70 – Production and Process Controls**
  - Applies to processes like secure firmware installation, device imaging, and supply chain security
  - Ensures secure configuration is maintained throughout manufacturing
- **820.100 – Corrective and Preventive Actions (CAPA)**
  - Vulnerabilities discovered postmarket (e.g., via penetration testing or CVE reports) must be investigated and addressed
  - Security incidents must trigger risk reassessment and documented remediation
- **820.198 – Complaint Handling**

- Complaints that involve cybersecurity-related performance failures or safety issues must be logged and investigated
- Ties into incident response processes described in FDA postmarket guidance

➢ **820.200 – Servicing**

- Ensures that software patches, firmware updates, and field servicing activities are securely managed, tracked, and validated

## 2.8 HIPAA & GDPR – Privacy and Data Security Regulations

These two regulations define how protected health information (PHI or personal data) must be handled, stored, transmitted, and safeguarded — including when processed or stored by medical devices or their connected ecosystems (e.g., apps, cloud platforms, remote monitoring tools).

| Regulation | Jurisdiction | Scope |
|---|---|---|
| **HIPAA – Health Insurance Portability and Accountability Act** | United States | Protects electronic Protected Health Information (ePHI) |
| **GDPR – General Data Protection Regulation** | European Union | Protects personal data, including health-related data |

### Why They Matter for Medical Device Cybersecurity:

Medical devices that store, transmit, or interact with patient data must secure that data according to applicable privacy laws. Even if the device is physically secure, improper data handling can lead to breaches, regulatory fines, and patient harm.

*Referenced in:*

- FDA Postmarket Cybersecurity Guidance (2016)
- MDCG 2019-16 (EU Medical Device Cybersecurity Guidance)
- IMDRF Cybersecurity Principles and Practices (2020)

### HIPAA Security Rule Requirements (U.S.)

Under HIPAA, medical device data (if it contains ePHI and is used by or on behalf of covered entities) must be protected via:

- **Access Controls:** Ensure only authorized users can view or modify patient data
- **Audit Controls:** Device or system must log access and changes to ePHI
- **Integrity Controls:** Mechanisms to ensure data is not altered or destroyed in an unauthorized manner
- **Transmission Security:** ePHI must be encrypted when sent over networks
- **Security Management Process:** Risk analysis and mitigation activities must be documented

- **Breach Notification Rule:** Obligates disclosure to affected individuals and regulators if a breach occurs

*Source: HIPAA Security Rule (45 CFR §164.308–316)*

### GDPR Requirements (EU & Global Applicability)

Even non-EU companies must comply with GDPR if they **process personal data of EU citizens**, including through connected devices or cloud platforms.

- **Lawful Basis for Data Collection**: Must have patient consent or other legal basis
- **Data Minimization & Purpose Limitation**: Devices should only collect what's necessary
- **Right to Access & Erasure**: Users can request access to or deletion of their data
- **Data Protection by Design & by Default**: Security must be embedded from the design phase
- **Security of Processing (Article 32)**: Encryption, access control, breach response plans required
- **Breach Notification (Articles 33 & 34)**: Must notify authorities within 72 hours of discovery

*Source: GDPR Articles 5, 25, 32, 33, 34*

## 2.9 Global Regulations – MDR (EU), IMDRF, CMDE (China), MDCG

While the FDA governs medical device cybersecurity in the U.S., several international regulatory bodies have published their own guidance aligned with or complementary to FDA principles. Global manufacturers must account for these regulations when designing, submitting, and marketing medical devices worldwide

### MDR – Medical Device Regulation (European Union)

The EU MDR (Regulation (EU) 2017/745) governs the safety and performance of medical devices in Europe. It includes cybersecurity requirements under Annex I: General Safety and Performance Requirements (GSPR).

*Reference: EU MDR Official Text*

- **Cybersecurity Focus Areas:**
  - Devices must be designed and manufactured to ensure protection against unauthorized access
  - Cybersecurity must be considered in risk management, software validation, and postmarket surveillance
  - Requires technical documentation addressing security measures
- **Aligned with:**
  - ISO 14971, IEC 62304, MDCG 2019-16

### IMDRF – International Medical Device Regulators Forum

The IMDRF is a global consortium of regulators (FDA, EU, China, Japan, Australia, Canada, etc.) that develops harmonized guidance to align medical device regulations across countries.

*Reference: "Principles and Practices for Medical Device Cybersecurity" (2020)*

- **Cybersecurity Focus Areas:**
  - Emphasizes secure design, risk management, threat modeling, and coordinated vulnerability disclosure (CVD)
  - Advocates for lifecycle cybersecurity aligned with ISO 14971 and IEC 62304
  - Promotes international consistency in cybersecurity documentation and submissions

## CMDE – China's Medical Device Evaluation Center

The Center for Medical Device Evaluation (CMDE) under China's NMPA (formerly CFDA) has issued guidance on software and cybersecurity for medical devices marketed in China.

*Reference: "Guideline for the Technical Review of the Cybersecurity of Medical Devices (Draft)" – NMPA, 2021*

- **Cybersecurity Focus Areas:**
  - Requires risk analysis of cybersecurity threats and technical controls to mitigate risks
  - Submission documentation must include:
    - Security design features
    - Access controls
    - Data transmission protection
    - Update and patch mechanisms
- Aligned with:
  - ISO 14971, IEC 62304, and IMDRF principles.

## MDCG – Medical Device Coordination Group (EU)

MDCG is the European advisory body supporting implementation of the MDR and IVDR. It provides detailed guidance on compliance strategies for manufacturers.

*Reference: MDCG 2019-16 – Guidance on Cybersecurity for Medical Devices*

- **Cybersecurity Focus Areas:**
  - Reinforces that cybersecurity must be addressed during design, manufacturing, and postmarket surveillance
  - Encourages manufacturers to apply:
    - Secure software development (IEC 62304)
    - Risk management (ISO 14971)
    - Security verification and validation
- **Aligns with:**
  - EU MDR Annex I and calls out SBOM, access control, and encryption requirements

# Section 3: Premarket Cybersecurity

## 3.0 Overview: Regulatory Submissions & Security Relevance

### What Are 510(k), PMA, and De Novo Submissions?

These are the three primary FDA pathways for bringing a medical device to market in the United States. Each pathway has different risk classifications, regulatory burdens, and cybersecurity expectations.

### When Is Cybersecurity Required in FDA Submissions?

If the device:

- Is connected (wired or wireless)
- Includes software or firmware
- Stores or transmits patient data
- Can be updated postmarket
- Has interfaces with other systems (e.g., hospital networks, apps)

Then cybersecurity documentation is required in the premarket submission.

*Source: FDA Cybersecurity in Medical Devices – Final Guidance, 2023*

### 510(k) – Premarket Notification

A 510(k) is a premarket submission made to the FDA to demonstrate that a new device is "substantially equivalent" to a legally marketed predicate device (same intended use and similar technological characteristics).

Applies to:

- Most Class II devices (moderate risk)
- Some Class I devices (low risk) requiring clearance

Cybersecurity Relevance:
Devices submitted via 510(k) must now include cybersecurity documentation if they are connected, programmable, or contain software that could impact safety or effectiveness.

*Source: 21 CFR 807 Subpart E, FDA Cybersecurity Guidance for Premarket Submissions, 2023*

### PMA – Premarket Approval

A PMA is the most stringent type of device application, requiring scientific evidence to demonstrate safety and effectiveness.

Applies to:

- Class III devices (highest risk) — e.g., life-sustaining, implantable, or high-impact diagnostic devices.

Cybersecurity Relevance:
Because PMA devices are often critical, the FDA expects more comprehensive cybersecurity documentation, including full testing results, secure update validation, and incident response planning.

*Source: 21 CFR Part 814, FDA Guidance: Premarket Approval (PMA), Medical Devices*

## De Novo Classification Request

A De Novo submission is used when a manufacturer has a novel device with no predicate, but the device poses low to moderate risk and is appropriate for general or special controls.

Applies to:

- First-of-its-kind Class I or II devices
- Devices that do not qualify for 510(k) because no substantially equivalent device exists

Cybersecurity Relevance:
De Novo devices often involve new technology, which can introduce unique cybersecurity risks. The FDA expects manufacturers to proactively address these risks in the submission.

*Source: 21 CFR Part 860, FDA Guidance: De Novo Classification Process (2022)*

## Cybersecurity Items Required in a 510(k), PMA, or De Novo Submission

| Required Item | Description | Regulatory Alignment |
|---|---|---|
| **Threat Modeling** | Identify cybersecurity threats and attack paths (e.g., using STRIDE or MITRE ATT&CK) | FDA, ISO 14971 |
| **Cybersecurity Risk Assessment** | Analyze risks and mitigations, including safety impact | ISO 14971, FDA |
| **Security Design Requirements** | Document controls: access control, authentication, encryption, secure boot, etc. | FDA, IEC 62304 |
| **Software Bill of Materials (SBOM)** | List all software components (proprietary, open-source, third-party) and known CVEs | FDA, EO 14028, IMDRF |
| **Security Architecture** | Provide a diagram and narrative of system-level and data flow architecture, showing trust boundaries | FDA |
| **Security Testing & Verification** | Include results from static/dynamic analysis, fuzz testing, penetration testing, etc. | FDA, IEC 62304 |
| **Labeling for End Users** | Provide instructions related to cybersecurity use (e.g., password policies, update process) | FDA |

| | | |
|---|---|---|
| **Plan for Ongoing Security Management** | Describe postmarket plans: vulnerability disclosure, patching, update validation | FDA Postmarket Guidance |
| **Traceability Matrix** | Map threats → requirements → controls → testing evidence | FDA, ISO 14971 |

## Submission Formatting Tips

- **Use a Structured Cybersecurity Report**
  Create a single document or section that brings together all required content — clearly labeled and indexed.
- **Follow the Language in FDA Guidance**
  Use terminology and structure aligned with the 2023 FDA guidance (e.g., threat modeling, SBOM, risk assessment, security controls).
- **Include References to Standards**
  Where applicable, cite **ISO 14971, IEC 62304, NIST CSF**, or **IEC 62443** to show industry alignment.
- **Cross-Reference Other Submission Elements**
  Reference relevant sections of your **design dossier**, **V&V reports**, and **risk files** to avoid duplication and demonstrate traceability.
- **Ensure Consistency Across Documentation**
  Make sure SBOM entries match test results, risks are traceable to mitigations, and labeling is consistent with device capabilities.

# 3.1 Threat Modeling & Attack Surface Analysis

## What Is Threat Modeling?

Threat modeling is a structured process used to identify, prioritize, and mitigate potential cybersecurity threats early in the product development lifecycle. It allows manufacturers to anticipate how an attacker might exploit a system and design appropriate defenses.

- *Referenced in:*
  - FDA Premarket Cybersecurity Guidance, 2023
  - ISO 14971:2019 (Risk Management for Medical Devices)
  - NIST SP 800-154 – Guide to Data-Centric System Threat Modeling
  - IMDRF Principles and Practices for Cybersecurity (2020)

## Why It Matters in Medical Devices

The FDA expects manufacturers to analyze and document threats that could compromise the safety, effectiveness, or data integrity of a device. A comprehensive threat model helps define security requirements, guide control implementation, and support the risk management file submitted during regulatory review.

- Threats to assess may include:

- Unauthorized access or privilege escalation
- Data tampering or exfiltration
- Firmware injection or rollback
- Exploitation of wireless/network interfaces
- Abuse of APIs or physical service ports

## Common Threat Modeling Frameworks

| Framework | Purpose | Used For |
|---|---|---|
| **STRIDE** | Categorizes threats into: Spoofing (Impersonating users or devices), Tampering (Modifying code or data), Repudiation (Undeniable actions without audit trails), Information Disclosure (Unauthorized data exposure), Denial of Service (Blocking access or functionality), Elevation of Privilege (Gaining unauthorized permissions) | General device/system threat modeling |
| **MITRE ATT&CK** | Maps Known tactics and techniques used in healthcare and industrial attacks. Post-compromise actions, including lateral movement, persistence, and data exfiltration | Mapping postmarket vulnerabilities, threat intelligence |
| **DREAD** | Scores threats by: Damage potential, Reproducibility, Exploitability, Affected users, Discoverability | Prioritizing vulnerabilities (pre/postmarket) |

## Attack Surface Analysis

An attack surface is the total set of points through which an attacker could try to enter, exploit, or disrupt a system.

➢ Common Attack Surfaces in Medical Devices:

- Physical ports (USB, JTAG, serial)
- Wireless interfaces (Bluetooth, Wi-Fi, NFC, Zigbee)
- Mobile or companion apps
- Cloud platforms or APIs
- Network services (SSH, FTP, Telnet)
- Firmware update mechanisms
- User interfaces and input vectors

Manufacturers must identify all potential entry points, assess their exposure, and implement mitigations based on likelihood and impact.

*Reference: IMDRF Cybersecurity Guidance – 2020*

- *Threat modeling is referenced in:*
  - FDA Guidance on Premarket Cybersecurity Content
  - IEC 62443-3-3: System Security Requirements and Security Levels
  - NIST CSF – Identify Function (Asset and Risk Identification)

### Tools & Resources for Threat Modeling

- Microsoft Threat Modeling Tool: STRIDE-based diagramming
- OWASP Threat Dragon: Lightweight threat modeling for web-connected systems
- draw.io or Lucidchart: Custom threat/attack diagrams
- MITRE ATT&CK Navigator: Postmarket threat mapping (TTP tracking)

## 3.2 SBOM & Third-Party Component Analysis

### What Is an SBOM?

A Software Bill of Materials (SBOM) is a comprehensive list of all software components used in a medical device, including open-source, proprietary, and third-party libraries. It functions like a parts list for software, enabling manufacturers to track vulnerabilities, licensing, and maintenance requirements.

*Source: U.S. Executive Order 14028 – "Improving the Nation's Cybersecurity" (2021)*
*Regulatory Reference: FDA Cybersecurity Premarket Guidance (2023) – SBOM is required for submissions*

### Why SBOMs Are Critical in Medical Devices

- Supports vulnerability monitoring and CVE identification
- Helps evaluate risk from third-party components
- Required for FDA premarket cybersecurity documentation
- Enhances transparency across the software supply chain
- Enables faster incident response and patch prioritization

- *Referenced In:*
  - IMDRF Cybersecurity Principles (2020)
  - MDCG 2019-16 (EU Guidance)
  - NTIA & CISA SBOM Playbooks
  - NIST SP 800-218 (Secure Software Development Framework)

## What to Include in an SBOM

| Attribute | Description |
|---|---|
| **Component Name** | The library, package, or binary used |
| **Version** | Specific release number used in the build |
| **Supplier/Author** | Organization responsible for the component |
| **Dependency Relationship** | Parent/child relationships in nested libraries |
| **Licensing Info** | Open-source, proprietary, or commercial license |
| **Known Vulnerabilities (CVEs)** | Relevant Common Vulnerabilities and Exposures |

*Preferred Formats:* SPDX, CycloneDX, SWID

## SBOM Management Tools

| Tool | Purpose |
|---|---|
| **CycloneDX** | Lightweight SBOM format for embedded and enterprise systems |
| **SPDX (Linux Foundation)** | Widely used, supported by SPDX License List |
| **OWASP Dependency-Track** | Continuous CVE monitoring and SBOM management |
| **Anchore, Grype** | SBOM generation and container image scanning |
| **GitHub Advanced Security** | Alerts for vulnerable dependencies in repos |

## Submission Tips for FDA

- Include the SBOM as a machine-readable file in your premarket package
- Cross-reference SBOM entries in your risk assessment and testing plans
- Show how CVEs were addressed (mitigation, patching, justification for deferral)
- Maintain version control over SBOM during development and release cycles

# 3.3 Risk Assessment & Documentation

## What Is a Cybersecurity Risk Assessment?

A cybersecurity risk assessment identifies, evaluates, and prioritizes cyber threats that could compromise a medical device's safety, performance, or data integrity. It guides the selection of appropriate mitigations, controls, and design features and is required as part of FDA's premarket submissions.
*Source: ISO 14971:2019 – Application of Risk Management to Medical Devices*

➢ *Required by:*

- FDA Premarket Cybersecurity Guidance (2023)
- ISO 14971 (Risk Management)
- IEC 62304 (Software Lifecycle)
- 21 CFR Part 820 (Design Controls)

## Why It Matters in Premarket Submissions

The FDA requires that manufacturers evaluate cybersecurity threats that could lead to patient harm, not just data loss. These assessments must be:

- Risk-based
- Well-documented
- Traceable to mitigations and test results

## Core Risk Management Elements (ISO 14971 Aligned)

| Step | Purpose | Tools/Examples |
|---|---|---|
| **1. Hazard Identification** | Determine how cybersecurity threats could cause harm | Threat modeling, attack surface review |
| **2. Risk Analysis** | Evaluate severity & likelihood of harm if a threat is exploited | CVSS scoring, clinical impact modeling |
| **3. Risk Evaluation** | Decide if the risk is acceptable or needs mitigation | Risk acceptability matrix |
| **4. Risk Control Measures** | Define and implement mitigations (technical + procedural) | Encryption, secure boot, access control |
| **5. Residual Risk Analysis** | Re-assess remaining risk after mitigation | Consider layered defense and compensating controls |
| **6. Risk-Benefit Analysis** | Justify high residual risk (if necessary) | Clinical utility vs. mitigation burden |
| **7. Documentation & Traceability** | Show full traceability in submission package | Risk tables, traceability matrix, test plans |

## What Documentation Should Be Submitted to the FDA?

✓ **Risk Assessment Summary**

- Identify threats, mapped to potential harms
- Describe risk controls and rationale
- Include severity, probability, and residual risk scoring

✓ **Traceability Matrix**

- Map each identified risk → mitigation → test case
- Demonstrates systematic security control coverage

✓ **Risk Acceptability Criteria**

- Define criteria for “acceptable” residual risk (e.g., risk rating ≤ Medium)
- Aligned with ISO 14971 Annex D

✓ **Risk-Benefit Justification (if needed)**

- Document why certain risks may remain (e.g., clinical tradeoff, infeasibility of mitigation)

✓ **Link to Design Controls**

- Connect to 21 CFR 820.30 – Design validation and verification
- Include V&V reports supporting mitigation effectiveness

### Risk Scoring Tools and References

| Standard/Tool | Purpose |
|---|---|
| **ISO 14971** | Defines full risk management process for medical devices |
| **CVSS (Common Vulnerability Scoring System)** | Technical exploitability scoring for software flaws |
| **FDA 2023 Guidance – Table 3** | Sample framework for cybersecurity risk acceptability |
| **MITRE CWE/CVE** | Tracks software weaknesses and vulnerabilities |
| **NIST 800-30** | General guidance for conducting IT/cyber risk assessments |

## 3.4 Secure SDLC & IEC 62304 Compliance

### What Is the Secure SDLC?

A Secure Software Development Lifecycle (Secure SDLC) is the integration of security-focused activities into every phase of software development, from requirements gathering through release and maintenance. For medical devices, it must align with IEC 62304, the global standard for medical device software lifecycle processes.

✓ *Referenced in:*

- FDA Premarket Cybersecurity Guidance (2023)
- IEC 62304 – Medical Device Software Lifecycle
- IMDRF Cybersecurity Guidance (2020)
- EU MDR & MDCG 2019-16 (EU)

### Why It Matters in Premarket Submissions?

FDA requires manufacturers to show that security was considered and implemented throughout the software lifecycle. This includes:

- Secure requirements gathering
- Implementation of mitigations
- Verification and validation (V&V)

- Postmarket update planning

*FDA Source:*

*"Cybersecurity activities should be incorporated into the software development and quality system processes throughout the device lifecycle."*
*— FDA Cybersecurity Guidance, 2023*

## IEC 62304 Stages and Security Activities

| SDLC Phase (IEC 62304) | Secure SDLC Focus |
|---|---|
| **Software Planning** | Define cybersecurity objectives, architecture, development environment, and tools |
| **Requirements Analysis** | Document security requirements based on threat modeling and risk assessment |
| **Design** | Specify architecture-level controls (authentication, secure data storage, OTA updates) |
| **Implementation** | Apply secure coding practices and development standards (e.g., OWASP, CERT) |
| **Verification & Testing** | Perform SAST, DAST, fuzzing, pen testing, and security feature validation |
| **Release** | Ensure security controls are fully implemented, tested, and documented |
| **Maintenance** | Plan for vulnerability monitoring, patching, and incident response postmarket |

## Key Secure Coding & Testing Practices

✓ Secure Coding Standards
- Use OWASP Secure Coding Guidelines, MISRA, or CERT C/C++ for embedded systems
- Avoid common flaws: buffer overflows, hardcoded credentials, improper input handling

✓ Static Application Security Testing (SAST)
- Analyze source code for vulnerabilities before execution
- Tools: SonarQube, Fortify, CodeSonar

✓ Dynamic Application Security Testing (DAST)
- Test running application behavior and responses
- Tools: Burp Suite, OWASP ZAP, Postman

✓ Fuzz Testing
- Input malformed data to uncover crashes or logic flaws
- Tools: Peach Fuzzer, BooFuzz, LLVM libFuzzer

✓ Penetration Testing

- Simulate real-world attacks to evaluate system defenses
- Often required for FDA documentation

✓ Secure Update Process Validation

- Test digital signature verification, rollback prevention, and update integrity
- Required under IEC 62304 + FDA guidance

### Submission Documentation Checklist

Include the following in your FDA submission package:

- ✓ Secure software design documentation
- ✓ Verification & validation reports for security features
- ✓ Secure coding standards used
- ✓ Results of SAST, DAST, fuzzing, and pen testing
- ✓ Software maintenance and patching plans
- ✓ Integration with risk assessment and traceability matrix

## 3.5 Device & Communications Security Controls

### Why Security Controls Matter

The FDA requires medical devices to implement technical safeguards that protect against unauthorized access, data tampering, and unsafe behavior. These controls must be based on risk assessment outcomes, threat modeling, and aligned with secure design principles.

➢ *Referenced in:*

- FDA Premarket Cybersecurity Guidance (2023)
- IEC 62443-4-2 (Embedded Device Security)
- MDCG 2019-16 (EU Cybersecurity Guidance)
- ISO 14971 & IEC 62304

### Designing Device-Level Security Controls

These controls must be integrated into the device architecture and software design, validated during V&V testing, and documented in premarket submissions.

1. **Authentication Mechanisms**

- Unique user accounts and role-based access control (RBAC)
- Support for strong passwords, key-based auth, or certificates
- Multi-factor authentication (MFA) for service personnel or admin roles
- Secure storage of credentials (e.g., salted hashes, TPM, HSM)

*Standards: IEC 62443-4-2, NIST SP 800-63*

2. **Data Encryption**
   - At rest: Encrypt sensitive data stored on device (e.g., AES-256, FIPS 140-2 validated)
   - In transit: Encrypt all communications using TLS 1.3, IPsec, or VPN
   - Key management: Secure generation, storage, rotation, and destruction of encryption keys

*Standards: NIST SP 800-57, FIPS 140-2, IEC 62443*

3. **Secure Boot and Firmware Integrity**
   - Validate firmware integrity during boot using cryptographic signatures
   - Prevent rollback to vulnerable firmware versions
   - Implement write-protection and anti-tampering checks

*Required by: FDA, IEC 62443-4-2, IMDRF Cybersecurity Guidance*

4. **Secure Update Mechanisms**
   - Digitally sign all software/firmware updates
   - Validate update source and signature before install
   - Enforce rollback protection and audit update results
   - Ensure secure delivery channel (e.g., encrypted, authenticated)

*Refer to: IEC 62304 (Maintenance), FDA Postmarket Guidance*

## Communications Security Controls

These apply to all interfaces used by the device — wired, wireless, cloud, and mobile.

1. **Network Protocol Hardening**
   - Disable unused ports and protocols
   - Enforce TLS 1.3 for all IP-based communications
   - Use firewall rules, IP filtering, and MAC address restrictions
2. **Wireless Security**
   - Secure Bluetooth LE pairing and bonding (e.g., authenticated, encrypted)
   - Use WPA3 for Wi-Fi modules

- Secure Zigbee or proprietary RF protocols with AES encryption and nonce validation
- Monitor for RF-based attacks (e.g., jamming, replay)

*Guidance: NIST SP 800-121 (Bluetooth), IEC 62443, FDA*

3. **API & Interface Security**
    - Authenticate all API access (OAuth2, API keys, JWT)
    - Input validation and rate limiting
    - Enforce HTTPS with HSTS and certificate pinning
    - Disable debug or dev interfaces in production firmware
4. **TLS & Certificate Management**
    - Support latest TLS versions (1.3 or 1.2 minimum)
    - Use strong cipher suites
    - Validate certificates and expiration
    - Rotate device certs securely (e.g., during update or provisioning)

### FDA Submission Expectations

- ✓ Security architecture diagram (with trust boundaries)
- ✓ Description of each implemented control
- ✓ Test results validating encryption, auth, secure boot, update process
- ✓ Mapping to identified threats and risks
- ✓ Explanation of residual risks (if any)

## 3.6 Traceability Matrix Development

### What Is a Traceability Matrix?

A traceability matrix is a structured tool that shows the relationship between cybersecurity elements such as:

- Identified threats and risks
- Defined security requirements
- Implemented controls and mitigations
- Associated verification and validation (V&V) evidence

This matrix ensures that each threat has been addressed, and that every control has been tested and documented — providing a clear, auditable trail for regulatory reviewers.

➢ *Referenced in:*

- FDA Cybersecurity Guidance (2023)
- ISO 14971:2019 – Risk Management
- IEC 62304 – Software Lifecycle
- IMDRF Cybersecurity Principles (2020)

## Why It Matters in FDA Submissions

The FDA explicitly calls for a traceability matrix to help reviewers confirm that all cybersecurity threats identified in threat modeling are traced to mitigations and evidence of effectiveness.

*Source: "Include a traceability matrix that maps threats and vulnerabilities to risk mitigations and design controls." — FDA Premarket Cybersecurity Guidance, 2023*

## Recommended Columns for a Cybersecurity Traceability Matrix

| Element | Example | Purpose |
|---|---|---|
| **Threat ID** | T-001 | Matches threat modeling outputs (e.g., STRIDE, MITRE) |
| **Threat Description** | "Unencrypted network traffic" | Summarizes the cybersecurity threat |
| **Risk ID / Hazard** | R-01 / Loss of data confidentiality | Linked to ISO 14971 risk analysis |
| **Security Requirement** | REQ-ENCRYPT-01 | Defines what the system must do (e.g., use TLS 1.3) |
| **Mitigation / Control** | Implement TLS 1.3 with cert validation | Technical or procedural control applied |
| **Verification Method** | DAST, Pen Test, SCA Tool | How the control was validated |
| **Test Evidence** | Report-PT-2023-08, Test ID V-004 | Reference to test case or V&V documentation |
| **Residual Risk Level** | Low | Based on post-control ISO 14971 analysis |

## Tools You Can Use

| Tool | Functionality |
|---|---|
| **Excel / Google Sheets** | Simple, flexible, widely accepted by FDA reviewers |
| **IBM DOORS / Jama Connect** | Formal requirements management and traceability platforms |
| **MedTech PLM Tools** | Often support integration with IEC 62304, ISO 14971 workflows |

| | |
|---|---|
| **Custom Templates** | May be created based on design control file format and submission strategy |

## Tips for Strong FDA-Ready Traceability

- ✓ Tips for Strong FDA-Ready Traceability
- ✓ Maintain consistent IDs across threat modeling, requirements, risk assessment, and testing
- ✓ Cross-reference your SBOM if specific components are linked to certain threats or mitigations
- ✓ Group traceability matrix entries by system component, interface, or data flow
- ✓ Include this matrix in your cybersecurity submission package, not buried within broader V&V reports
- ✓ Align residual risk scoring with your defined acceptability criteria (see Section 3.3)

# 3.7 Cybersecurity Labeling & Human Factors

## What Is Cybersecurity Labeling?

Cybersecurity labeling refers to the information provided to users, administrators, and service personnel about how to securely operate and maintain the medical device. It is part of the device's Instructions for Use (IFU) and may also include technical manuals, quick-start guides, or web-based support documentation.

➢ *Referenced in:*

- FDA Premarket Cybersecurity Guidance (2023)
- 21 CFR Part 801 – Device Labeling
- IEC TR 60601-4-5 – Guidance on Usability for Networked Devices
- IMDRF Cybersecurity Guidance (2020)

## Why Labeling Matters for Cybersecurity

Proper cybersecurity labeling helps ensure users:

- Operate the device within safe and secure configurations
- Understand their roles and responsibilities (e.g., password management, update processes)
- Avoid configurations that expose the device to cyber threats
- Comply with clinical and IT security protocols in healthcare settings

FDA Source: "Manufacturers should provide information in device labeling to help users manage cybersecurity risks." — FDA Cybersecurity Guidance, 2023

## What to Include in Cybersecurity Labeling

| Labeling Element | Purpose |
|---|---|
| **Default Credentials** | List default usernames/passwords and require change upon first use |

| | |
|---|---|
| **Access Control Guidance** | Explain user roles, permissions, and how to manage access |
| **Network Configuration Requirements** | Describe necessary security settings (e.g., firewalls, Wi-Fi security, VLANs) |
| **Software Update Process** | Instructions for installing patches, validating updates, and rollback protection |
| **Physical Security Recommendations** | Describe port locks, tamper seals, and device access controls |
| **Known Limitations or Residual Risks** | Inform users of any limitations (e.g., unsupported protocols, unpatched features) |
| **Support Contact Info** | Provide guidance on how to report security issues or suspected vulnerabilities |
| **Reference to SBOM (if applicable)** | Optionally include public-facing SBOM or update link for transparency |

### Integrating Human Factors into Cybersecurity Design

Human factors engineering (HFE) helps ensure cybersecurity features are usable, understandable, and error-resistant — especially for non-technical users such as clinicians or patients.

| Design Area | Human Factors Goal |
|---|---|
| **Password Prompts** | Use clear language and avoid requiring complex input steps |
| **Update Notifications** | Use intuitive alerts and simple steps to install updates |
| **Access Control Settings** | Avoid nested or confusing interfaces for setting user roles |
| **Security Warnings** | Ensure alerts are visible, actionable, and do not induce alarm fatigue |

*Reference: IEC TR 60601-4-5 – Guidance on safety and usability for connected medical devices*

## 3.8 Postmarket Readiness Plan (Premarket Deliverable)

### What Is a Postmarket Readiness Plan?

A Postmarket Cybersecurity Readiness Plan outlines how the manufacturer will monitor, manage, and respond to cybersecurity threats after the device is on the market. The FDA expects this to be included as part of the premarket submission for connected or software-based medical devices.

- *Referenced in:*
  - FDA Postmarket Cybersecurity Guidance (2016)
  - FDA Premarket Cybersecurity Guidance (2023)
  - ISO/IEC 30111 & 29147 (Vulnerability Handling & Disclosure)

- IMDRF Cybersecurity Principles (2020)

## Why This Is Required in Premarket Submissions

The FDA requires manufacturers to show they have:

- A plan for vulnerability monitoring and handling
- A process for patching and software updates
- A method for coordinated vulnerability disclosure (CVD)
- Procedures to evaluate, mitigate, and communicate risks postmarket

*FDA Source: "Sponsors should include a plan for how postmarket cybersecurity activities will be conducted, including vulnerability management and coordinated disclosure." — FDA Cybersecurity Guidance, 2023*

## Core Elements of a Postmarket Readiness Plan

| Component | Description |
|---|---|
| **Vulnerability Monitoring Process** | Use CVE databases, threat intel feeds (e.g., NVD, ICS-CERT) to monitor for new vulnerabilities in device components |
| **Risk Re-Evaluation Protocol** | Reassess ISO 14971 risk if new vulnerabilities could affect safety or effectiveness |
| **Remediation Planning** | Define patching process, impact assessment, regression testing, and validation procedures |
| **Secure Update Delivery** | Ensure patch delivery is authenticated, validated, and logged; support rollback if needed |
| **Coordinated Vulnerability Disclosure (CVD)** | Provide public contact for security researchers; follow ISO 30111 & ISO 29147 |
| **Communication Plan** | Explain how users and regulators will be notified of patches, risks, or workarounds |
| **Integration with CAPA and Complaint Handling** | Postmarket threats and vulnerabilities must feed into existing quality system (21 CFR Part 820.100 & 820.198) |

## How to Document It in Your Submission

Include a section or appendix titled *"Postmarket Cybersecurity Plan"* in your FDA submission
Describe:

- How you will monitor for vulnerabilities (tools, processes, roles)
- Your criteria for patching vs. monitoring vs. workaround
- Your timeline targets for remediation (e.g., within 30 days for critical CVEs)
- How you will handle responsible disclosure and MDR/recall triggers
- Links to your risk assessment and traceability matrix

Reference relevant standards (ISO 30111, ISO 14971, FDA Postmarket Guidance)

# Section 4: Postmarket Cybersecurity

## 4.0 Overview: Postmarket Cybersecurity Lifecycle

### What Is Postmarket Cybersecurity?

Postmarket cybersecurity refers to the ongoing activities a manufacturer performs after a medical device has been released to detect, evaluate, mitigate, and report cybersecurity vulnerabilities or incidents. These efforts are critical for ensuring that the device continues to meet safety, effectiveness, and regulatory requirements throughout its usable life.

### Key Objectives of Postmarket Cybersecurity

- Monitor for newly discovered vulnerabilities, threats, and exploits
- Evaluate and re-assess cybersecurity risks in light of new information
- Implement timely mitigations (e.g., patches, workarounds)
- Communicate with regulators, customers, and affected users
- Improve processes through incident response, CAPA, and surveillance feedback

➢ *Referenced in:*
- FDA Postmarket Management of Cybersecurity in Medical Devices (2016)
- 21 CFR Part 820 (Quality System Regulation)
- ISO 14971 (Risk Management)
- IMDRF Cybersecurity Principles (2020)
- MDCG 2019-16 (EU Guidance)

### Regulatory Expectations

The FDA and other global regulators expect manufacturers to integrate cybersecurity into their postmarket surveillance systems, including:

| Requirement | Source |
|---|---|
| **Vulnerability monitoring & risk evaluation** | FDA Postmarket Guidance (2016), ISO 14971 |
| **Timely remediation & secure updates** | FDA, IEC 62304, ISO/IEC 30111 |
| **Reporting of incidents or patient-impacting vulnerabilities** | FDA MDR, EU MDR, IMDRF |
| **Coordinated vulnerability disclosure (CVD)** | ISO/IEC 29147, ISO/IEC 30111 |
| **Quality system integration (CAPA, complaint handling)** | 21 CFR Part 820 |

### Lifecycle Integration

Postmarket cybersecurity is not a standalone activity — it is tightly integrated with:
- Premarket planning (see Section 3.8)
- Design controls and risk management (21 CFR 820.30, ISO 14971)
- Complaint handling and corrective actions (21 CFR 820.198 & 820.100)

- Software maintenance and update procedures (IEC 62304)

A mature postmarket security process ensures that patient safety is maintained even as the threat landscape evolves, device configurations change, and vulnerabilities emerge over time.

## 4.1 Vulnerability Monitoring & Threat Intelligence

### What It Is

Vulnerability monitoring and threat intelligence involve the ongoing identification of new cybersecurity threats, weaknesses, and attack methods that may affect a marketed medical device or its ecosystem (e.g., cloud, mobile app, network integration).

These practices enable manufacturers to act proactively updating risk assessments, issuing patches, and notifying users when necessary.

➢ *Referenced in:*

- FDA Postmarket Cybersecurity Guidance (2016)
- ISO 14971 – Risk Management
- IMDRF Cybersecurity Guidance (2020)
- MDCG 2019-16 (EU)

### Why It's Required

The FDA expects manufacturers to continuously monitor for emerging vulnerabilities that could compromise device safety or effectiveness. Monitoring is part of a postmarket surveillance program and helps trigger risk re-evaluation and mitigation.

*FDA Source: "Manufacturers should have a process for actively monitoring cybersecurity information sources to identify and assess vulnerabilities relevant to their devices." — FDA Postmarket Cybersecurity Guidance, 2016*

### What to Monitor

| Target | Examples |
|---|---|
| **Software components (from SBOM)** | Open-source libraries, OS, drivers, communication stacks |
| **Embedded firmware or device OS** | RTOS, Linux distros, Bluetooth stacks, TCP/IP libraries |
| **Cloud and mobile ecosystems** | APIs, SDKs, hosting platforms, companion apps |
| **Hardware-level exploits** | USB stack vulnerabilities, DMA attacks, side-channel threats |
| **Supply chain components** | 3rd-party modules, chips, or OEM software |

### Sources of Threat Intelligence & Vulnerability Data

| Source | Purpose |
|---|---|
| **NVD (National Vulnerability Database)** | CVE feeds with CVSS scoring, vendor data |
| **ICS-CERT (CISA)** | Advisories specific to industrial and medical systems |
| **FDA Recalls & Safety Communications** | Alerts about patient-impacting vulnerabilities |
| **Vendor Security Bulletins** | OS and software vendor advisories (e.g., Microsoft, Google, Philips) |
| **OpenSSF & OSV Scanner** | Vulnerabilities in open-source components |
| **MITRE CVE & CWE Databases** | Public vulnerability and weakness classification |
| **Commercial Tools (optional)** | Rapid7, Tenable, ThreatConnect, VulnDB, Recorded Future |

### Tools for Monitoring

| Tool | Use Case |
|---|---|
| **Dependency-Track** | Monitors SBOM components and alerts on CVEs |
| **Grype / Syft** | Generates and scans SBOMs for vulnerabilities |
| **CycloneDX** | SBOM format supporting CVE lookup and threat metadata |
| **SIEM tools (e.g., Arctic Wolf, Splunk)** | Real-time log monitoring, threat correlation |
| **CVE-as-a-Service APIs** | Automate monitoring workflows with real-time feeds (NVD, OSV, CVE.org) |

### Submission and Documentation Tips

- Include your vulnerability monitoring strategy in the postmarket plan submitted during premarket (see Section 3.8)
- Document tools, roles, and procedures for how monitoring is performed
- Establish a review cadence (e.g., weekly/monthly checks + event-based monitoring for high-profile CVEs)

## 4.2 Vulnerability Triage & Risk Re-Evaluation

### What It Is

Vulnerability triage is the structured process of evaluating newly discovered vulnerabilities and deciding whether they pose a safety or effectiveness risk to a marketed medical device. It includes assessing technical severity, clinical impact, and potential patient harm.

This process is followed by risk re-evaluation, where the vulnerability is analyzed using your existing ISO 14971-aligned risk management process to determine if mitigation is needed.

➢ *Referenced in:*

- FDA Postmarket Cybersecurity Guidance (2016)

- ISO 14971:2019 – Risk Management for Medical Devices
- IMDRF Cybersecurity Guidance (2020)
- MDCG 2019-16 (EU Cybersecurity Guidance)

## Why It Matters

The FDA expects manufacturers to perform a timely and documented assessment of every vulnerability that could affect the device.
If a vulnerability creates uncontrolled risk, the manufacturer must implement and document mitigations (e.g., patch, update, communication, or recall).

*FDA Source: "Manufacturers should assess the impact of the vulnerability on the device functionality and the potential for patient harm, and determine whether additional actions are needed." — FDA Postmarket Cybersecurity Guidance, 2016*

## Key Triage Questions

- Does the vulnerability affect a component used in the device (via SBOM)?
- Is the component used in a security-critical function (e.g., auth, comms, update)?
- Can the vulnerability be exploited in the field based on current configurations?
- What is the CVSS score and has it been weaponized/exploited in the wild?
- Could exploitation result in patient harm or clinical disruption?

## Risk Re-Evaluation Process (ISO 14971 Aligned)

| Step | Description |
|---|---|
| **Hazard Re-Identification** | Assess if the vulnerability introduces a new or altered hazard |
| **Hazardous Situation Analysis** | Determine how the vulnerability could lead to unsafe use |
| **Risk Estimation** | Evaluate probability (e.g., exploitability) and severity (e.g., patient impact) |
| **Risk Evaluation** | Compare against acceptability thresholds |
| **Risk Control Decision** | Decide if patching, mitigation, or communication is needed |
| **Residual Risk Assessment** | Confirm residual risk is acceptable after action taken |
| **Documentation** | Log all triage steps and decisions in QMS (e.g., CAPA, risk file updates) |

## Prioritization Frameworks

Use a mix of technical severity + clinical impact for triage decisions:

- CVSS v3.x Score: Exploitability, impact metrics
- MITRE CWE/CVE: Classification of weakness
- FDA Risk Matrix: Combines likelihood + severity of harm

- Exploit Status: Known active exploit = higher urgency
- Affected Systems: Evaluate based on device role and network context

### Best Practices for Documentation

- Maintain a Vulnerability Intake & Triage Log
- Record all decisions, scoring, and re-evaluation justifications
- Link to the original SBOM component, CVE, and test data (if available)
- Update the ISO 14971 risk file with new hazard analysis if applicable
- Trigger CAPA if patient safety could be impacted

## 4.3 Remediation, Patching, and Update Validation

### What It Is

Remediation refers to the actions taken to mitigate or eliminate identified cybersecurity vulnerabilities, including applying software patches, configuration changes, or workarounds. Patching and update validation ensure that fixes are applied securely, reliably, and without introducing new risks to patient safety or device functionality.

➢ *Referenced in:*

- FDA Postmarket Cybersecurity Guidance (2016)
- IEC 62304 – Software Lifecycle
- IMDRF Cybersecurity Guidance (2020)
- ISO/IEC 30111 – Vulnerability Remediation
- 21 CFR Part 820 – Design Controls & CAPA

### Why It Matters

The FDA expects manufacturers to:

- Timely address uncontrolled risks due to vulnerabilities
- Validate that updates are effective, secure, and do not degrade device performance
- Maintain documentation of the update process, testing, and release controls

*FDA Source: "Manufacturers should remediate vulnerabilities that present an uncontrolled risk and validate the update using appropriate methods." — FDA Postmarket Cybersecurity Guidance, 2016*

### Key Steps in the Remediation Process

| Step | Activity |
|---|---|
| **1. Determine Remediation Type** | Patch, workaround, configuration update, or disable feature |
| **2. Develop Fix** | Use secure SDLC process, code reviews, build/test environments |

| | |
|---|---|
| **3. Validate Update** | Functional, regression, and security testing; verify fix does not impair device safety |
| **4. Digitally Sign and Package** | Apply cryptographic signing, version control, and audit metadata |
| **5. Deploy Securely** | OTA update, local USB installer, or HCP-driven update process |
| **6. Confirm Delivery and Success** | Post-deployment validation, logs, success confirmation |
| **7. Document and Close** | Finalize CAPA, update risk file, notify stakeholders if needed |

## Secure Update Requirements

| Requirement | Details |
|---|---|
| **Cryptographic Signing** | Use private/public key pair to sign and verify update authenticity |
| **Rollback Protection** | Prevent older, vulnerable versions from being reinstalled |
| **Integrity Verification** | Use hash checks or digital signatures for tamper detection |
| **Secure Transport** | Deliver updates via TLS 1.2+ or secure offline channels |
| **Audit Logging** | Log update event, timestamp, version, and user actions |

*Aligns with: IEC 62304, IEC 62443-4-2, FDA & IMDRF guidance*

## Update Validation Methods

- Unit testing: Ensure bug fixes behave as expected
- Regression testing: Confirm existing features are unaffected
- Security testing: Re-check CVE/weakness closure (e.g., via SAST, pen testing)
- Hardware-in-the-loop simulation (for embedded devices)
- Mock clinical workflow testing (to validate safety in real-world scenarios)

## Document Everything

- Patch or update rationale
- V&V results and validation protocol
- Rollback plan and secure install record
- Update instruction for end users / IT admins
- Notification of affected users (if needed)

If risk remains high or a fix is not feasible, initiate risk communication and MDR reporting (see Section 4.5).

## 4.3 Coordinated Vulnerability Disclosure (CVD)

### What Is CVD?

Coordinated Vulnerability Disclosure (CVD) is the process of publicly documenting and managing how a manufacturer handles externally reported security vulnerabilities in a responsible, timely, and collaborative way. This includes interactions with security researchers, customers, healthcare providers, and regulators.

CVD ensures vulnerabilities are addressed without causing unnecessary harm, and builds transparency and trust with the healthcare ecosystem.

➢ *Referenced in:*

- FDA Postmarket Cybersecurity Guidance (2016)
- ISO/IEC 29147 – Vulnerability Disclosure
- ISO/IEC 30111 – Vulnerability Handling Processes
- IMDRF Cybersecurity Guidance (2020)
- NTIA CVD Guidelines (U.S. Commerce Dept.)

### Why It Matters

The FDA encourages manufacturers to adopt formal CVD programs and consider them a "recognized best practice." If followed, CVD may reduce regulatory burden and even exempt the manufacturer from certain reporting requirements for minor, well-managed vulnerabilities.

*FDA Source: "Engaging in coordinated disclosure can demonstrate that a manufacturer has actively mitigated and managed risks." — FDA Postmarket Cybersecurity Guidance, 2016*

### Core Elements of a CVD Program

| Element | Description |
|---|---|
| **Public Contact Channel** | A dedicated email (e.g., security@company.com) or web form to report vulnerabilities |
| **Disclosure Policy** | Publicly available policy that outlines how reports will be handled and what to expect |
| **Acknowledgment Timeline** | Commit to acknowledging reports (e.g., within 5 business days) |
| **Triage and Investigation Workflow** | Internal SOP for intake, risk analysis, and response |
| **Researcher Recognition** | Optional hall of fame, thank-you notes, or bug bounty integration |
| **Disclosure Coordination** | Work with researchers and regulators to disclose vulnerabilities at the appropriate time |
| **Communication with Affected Users** | Issue bulletins, patches, or mitigations as needed |

## What to Include in Your CVD Policy Page

- Purpose and scope of the program
- Responsible disclosure expectations
- How to report (email/form, encryption key)
- What information to include in a report
- Timeline for acknowledgment and response
- Legal safe harbor / "no retaliation" language
- How you will communicate findings and remediation

## Supporting Tools

| Tool | Use |
|---|---|
| **Vulnogram / CVE Services** | Format and submit CVEs to MITRE/CVE.org |
| **Bugcrowd / HackerOne** | Platforms for bug bounty + CVD handling |
| **Encrypted Email (PGP)** | Secure vulnerability communication |
| **JIRA / Ticketing** | Track internal triage, CAPA, and resolution |
| **Public Advisory Templates** | Used for disclosure when patch is ready |

# 4.4 Incident Response & Regulatory Reporting

## What Is Incident Response?

Incident response (IR) is the structured approach a manufacturer takes to identify, contain, investigate, and resolve cybersecurity incidents involving a marketed medical device. This includes both real-world cyberattacks and confirmed exploitation of known vulnerabilities.

Regulatory reporting refers to the process of notifying government agencies (e.g., FDA, EU authorities) when an incident meets reporting thresholds related to patient safety, effectiveness, or public health risk.

➢ *Referenced in:*
- FDA Postmarket Cybersecurity Guidance (2016)
- 21 CFR Part 803 – Medical Device Reporting (MDR)
- ISO/IEC 27035 – Incident Response Standard
- IMDRF Cybersecurity Guidance (2020)
- EU MDR & MDCG 2021-27 (Vigilance & Cybersecurity Reporting)

## Why It Matters

Cybersecurity incidents can lead to device malfunction, data breaches, denial of therapy, or interrupted clinical care. These events must be handled promptly and transparently to protect patients, comply with regulations, and maintain public trust.

*FDA Source: "Manufacturers should have defined processes for incident response and criteria for reporting adverse events to the FDA." — FDA Postmarket Cybersecurity Guidance, 2016*

## Incident Response Process (ISO 27035-Aligned)

| Phase | Activity |
|---|---|
| **Preparation** | Build response plan, define roles, train team, establish playbooks |
| **Detection & Analysis** | Identify suspicious behavior, confirm incident, classify type and scope |
| **Containment** | Isolate affected device(s) or systems to limit further damage |
| **Eradication & Recovery** | Remove root cause (e.g., malware), apply patches, restore normal operations |
| **Post-Incident Activities** | Document response, update risk files, trigger CAPA, report to authorities if needed |

## When to Report to Regulators

- **US FDA (U.S.) – 21 CFR Part 803**
  - Report if the cybersecurity issue has caused or may cause death or serious injury, or if it requires a correction or removal of the product
  - This may include:
    - Compromised therapy delivery
    - Unauthorized access that impacts device function
    - Patch failure or ineffective mitigation
- **EU EU MDR & MDCG 2021-27**
  - Mandatory vigilance reporting if the incident led to or could have led to serious deterioration of health or death
  - Report to national competent authority within 2–15 days, depending on severity

## Who Else to Notify (if applicable)

- HCPs / Customers / Distributors
- Cybersecurity & Infrastructure Security Agency (CISA / ICS-CERT)
- MITRE CVE (if disclosing a vulnerability)
- Healthcare ISAC (H-ISAC)

Notification should include: device(s) affected, vulnerability details, risk, available mitigations, and timeline for remediation

## Tools & Resources

| Tool | Use |
|---|---|
| **SIEM (e.g., Splunk, Arctic Wolf)** | Event detection and response orchestration |
| **IR Playbooks / SOPs** | Step-by-step workflows for common incidents |

| | |
|---|---|
| **JIRA / CAPA Systems** | Track actions, decisions, root cause, and closures |
| **FDA eMDR Portal** | Online submission of MDR reports |
| **EU Manufacturer Incident Reports (MIR)** | Format for EU vigilance reporting (MDCG 2021-27) |

## 4.5 Postmarket Security Maintenance Plan

### What It Is

A Postmarket Security Maintenance Plan outlines how a manufacturer will sustain cybersecurity protections and respond to new threats over the full operational life of a medical device. This includes updating vulnerable components, continuing monitoring efforts, and preparing for the device's eventual end of support or decommissioning.

*Referenced in:*

- FDA Postmarket Cybersecurity Guidance (2016)
- IEC 62304 – Software Maintenance
- ISO 14971 – Risk Management
- IMDRF Cybersecurity Guidance (2020)
- MDCG 2019-16 – EU Guidance on Cybersecurity

### Why It's Important

Medical devices often remain in clinical use for years or even decades. Without a defined long-term security plan, outdated components or unsupported software can introduce patient safety risks, legal exposure, and noncompliance with regulators.

*FDA Source "Manufacturers should address cybersecurity throughout the product lifecycle, including after market release." — FDA Postmarket Cybersecurity Guidance, 2016*

### Key Components of a Security Maintenance Plan

| Component | Details |
|---|---|
| **Vulnerability Monitoring** | Continue CVE tracking, SBOM analysis, threat intel (see Section 4.1) |
| **Periodic Risk Reviews** | Reassess risk files annually or after new vulnerabilities emerge |
| **Component & Firmware Updates** | Plan for secure patching and configuration adjustments |
| **Cryptographic Maintenance** | Rotate certificates, deprecate weak algorithms (e.g., SHA-1) |
| **Documentation Updates** | Keep SBOM, risk files, and security architecture current |
| **CAPA Triggers** | Include security-related incidents and patching delays as triggers |
| **End-of-Life (EOL) Planning** | Define support timelines, final updates, and customer communication strategy |

## End-of-Life Cybersecurity Considerations

When a device reaches the end of its supported life:

- Notify customers in advance (12–24 months is common)
- Offer final firmware updates or mitigations
- Provide decommissioning guidance to ensure secure removal from networks
- Clearly state that future vulnerabilities will not be patched post-EOL
- Document these plans in regulatory filings and QMS artifacts

*Recommended by: IMDRF & FDA Lifecycle Security Principles*