Certified Specialist Programme in Medical Device Cybersecurity

Regulatory Framework for Medical Devices

Regulatory Framework for Medical Devices – Key Terms and Vocabulary

The regulatory environment governing medical devices is complex and continually evolving, especially as cybersecurity concerns become integral to device safety. Understanding the specific terminology used by authorities, manufacturers, and cybersecurity professionals is essential for anyone working in the Certified Specialist Programme in Medical Device Cybersecurity. The following explanation provides a comprehensive overview of the most important terms, organized by thematic groups. Each definition includes practical examples, typical applications in a cybersecurity context, and common challenges that professionals may encounter.

Medical Device – Any instrument, apparatus, implement, machine, appliance, implant, reagent, software, or related item intended for use in the diagnosis, prevention, monitoring, treatment, or alleviation of disease. Example: A programmable insulin pump that delivers medication based on sensor data. In cybersecurity, the device's software components become potential attack vectors, requiring protection of both the hardware and the embedded code.

Software as a Medical Device (SaMD) – Software that performs a medical purpose without being part of a physical device. Example: A mobile application that analyzes electrocardiogram data to detect atrial fibrillation. SaMD is subject to the same regulatory scrutiny as hardware devices, and its lifecycle includes continuous updates, which introduces unique security considerations such as version control and patch management.

Software in a Medical Device (SiMD) – Software that is integral to a medical device's functionality. Example: The firmware controlling the motor of an infusion pump. SiMD must be validated for safety and security, meaning that any vulnerability in the firmware can directly affect patient outcomes.

Risk Management – The systematic process of identifying, evaluating, controlling, and monitoring risks associated with a medical device. In the context of cybersecurity, risk management includes threat modeling, vulnerability assessment, and the implementation of mitigations. The ISO 14971 standard provides a framework for risk management, and many regulators require a risk management file that documents all identified risks, including those stemming from cyber threats.

Risk Management File (RMF) – A collection of documents that demonstrate how risks have been identified, analyzed, evaluated, and controlled throughout the device lifecycle. The RMF typically contains a risk analysis, risk evaluation, risk control measures, and a residual risk assessment. For cybersecurity, the RMF

must include a threat analysis that identifies potential attackers, attack vectors, and the impact of successful exploits.

Threat Analysis – The process of identifying potential sources of harm, such as malicious actors, and determining how they could exploit vulnerabilities. Example: Analyzing how a ransomware group could gain access to a hospital's networked ventilators. Threat analysis informs the development of security controls and is a required element of the risk management process.

Vulnerability – A weakness in a device's hardware, software, or operational environment that could be exploited to cause an undesirable outcome. Example: An unencrypted communication channel between a cardiac monitor and its central server. Vulnerabilities are identified through testing, code review, and penetration testing, and must be tracked in a vulnerability management system.

Residual Risk – The risk that remains after all feasible risk control measures have been implemented. In medical device cybersecurity, residual risk may be accepted if the benefit of the device outweighs the potential impact of a cyber incident, but it must be documented and justified.

Security Control – A safeguard or countermeasure that reduces the likelihood or impact of a security risk. Controls can be technical (e.G., Encryption, authentication), procedural (e.G., Security policies), or physical (e.G., Tamper-evident seals). Effective security controls are selected based on the risk assessment and must be validated for effectiveness.

Encryption – The process of converting data into a coded format that can only be read by authorized parties. Example: Using AES-256 to protect patient data transmitted from a wearable glucose sensor to a cloud service. Encryption is a critical control for protecting data confidentiality and integrity during storage and transmission.

Authentication – The verification of the identity of a user, device, or system. Example: Two-factor authentication required for remote access to the configuration interface of a surgical robot. Robust authentication mechanisms prevent unauthorized access and are a cornerstone of device security.

Authorization – The process of granting specific privileges to an authenticated entity. Example: A technician may be authorized to update firmware but not to change safety-critical parameters. Authorization controls ensure that users can only perform actions appropriate to their role.

Patch Management – The systematic process of applying updates to fix vulnerabilities, improve performance, or add functionality. In a medical device context, patches must be carefully validated to avoid unintended side effects. Regulatory bodies often require evidence that patches are applied in a controlled manner and that the impact on device safety is assessed.

Post-Market Surveillance (PMS) – Ongoing monitoring of a device after it has been placed on the market, aimed at detecting adverse events, performance issues, or emerging risks. Cybersecurity-related PMS

includes monitoring for new threats, collecting incident reports, and updating risk assessments. The FDA's Post-Market Management of Cybersecurity (PMM) guidance outlines expectations for manufacturers.

Adverse Event – Any undesirable experience associated with the use of a medical device. When a cyber incident leads to patient harm, it is classified as a cybersecurity-related adverse event. Example: A remote hacking incident that disables an insulin pump, resulting in hypoglycemia. Manufacturers must report such events to regulatory authorities.

Incident Report – Documentation of a security incident, including details of the attack, affected devices, impact, and corrective actions. Incident reports are a key component of PMS and may be submitted to agencies such as the FDA's MedWatch or the European Medicines Agency's EudraVigilance system.

Cybersecurity Incident – An event that compromises the confidentiality, integrity, or availability of a medical device or its data. Examples include unauthorized access, malware infection, denial-of-service attacks, and data breaches. Incidents must be investigated, mitigated, and reported according to regulatory requirements.

Threat Vector – The path or method by which a threat actor can gain access to a device. Common threat vectors for medical devices include wireless interfaces (Wi-Fi, Bluetooth), USB ports, legacy networking protocols, and insecure APIs. Understanding threat vectors is essential for designing effective security controls.

Attack Surface – The sum of all points where an unauthorized user could attempt to enter or extract data. Reducing the attack surface involves disabling unnecessary services, removing default credentials, and limiting network exposure. A smaller attack surface reduces the likelihood of successful exploitation.

Secure Development Lifecycle (SDL) – A structured process that integrates security activities into each phase of product development. The SDL includes threat modeling, secure coding practices, static and dynamic analysis, and security testing. Regulatory guidance increasingly expects manufacturers to follow an SDL to ensure cybersecurity is addressed early and continuously.

Static Application Security Testing (SAST) – Analysis of source code or binary files without executing the program, to find vulnerabilities such as buffer overflows or insecure APIs. Example: Using a SAST tool to scan the firmware of a pacemaker for unsafe memory handling. SAST is a proactive method for identifying flaws before deployment.

Dynamic Application Security Testing (DAST) – Testing that involves executing the application and interacting with it to discover runtime vulnerabilities. Example: Performing DAST on a web-based interface of a radiology workstation to detect SQL injection points. DAST complements SAST by revealing issues that only appear during operation.

Penetration Testing – Simulated attacks performed by security professionals to evaluate the effectiveness of

security controls. Penetration testing of medical devices may involve network scanning, protocol fuzzing, and exploitation of known vulnerabilities. Findings must be documented, remediated, and retested.

Fuzz Testing (Fuzzing) – An automated technique that supplies random or malformed inputs to a program to discover crashes or unexpected behavior. Fuzzing is especially useful for protocols used by medical devices, such as DICOM or HL7, where malformed messages could cause denial-of-service or data corruption.

Supply Chain – The network of organizations, processes, and resources involved in the creation and delivery of a medical device. The supply chain includes component manufacturers, software vendors, integrators, and distributors. Cybersecurity risks can arise at any point, such as compromised firmware from a third-party supplier.

Supply Chain Risk Management (SCRM) – The practice of identifying, assessing, and mitigating risks associated with the supply chain. SCRM for medical devices includes vetting suppliers, requiring security certifications, and conducting audits. Regulatory standards such as IEC 62443 emphasize the need for SCRM.

IEC 62443 – An international series of standards for industrial automation and control system security. Although originally designed for industrial environments, IEC 62443 is increasingly applied to medical device cybersecurity, providing a framework for defining zones, conduits, and security levels.

Zone – A logical grouping of assets that share common security requirements. In a hospital setting, a zone might consist of all devices that communicate over a dedicated network segment. Zoning helps to isolate critical devices and limit the spread of an attack.

Conduit – A controlled pathway that connects zones, allowing data to flow securely between them. Example: A firewall that mediates traffic between a clinical device zone and the hospital's enterprise network. Conduits enforce security policies and can include inspection, filtering, and logging.

Security Level (SL) – A measure of the robustness of security controls, ranging from SL1 (lowest) to SL4 (highest) in IEC 62443. The appropriate SL is determined based on risk assessment. For a life-supporting device, a higher SL (e.G., SL3 or SL4) may be required to protect against sophisticated threats.

Security by Design – An approach that incorporates security considerations from the earliest stages of product development, rather than adding them as an afterthought. Security by design involves threat modeling, secure coding, and architecture reviews. Regulators increasingly expect evidence of this approach in submissions.

Security by Default – Configuring a device with the most secure settings out of the box, minimizing the need for end-users to make security decisions. Example: Shipping a ventilator with all default passwords changed, network ports disabled, and encryption enabled. This reduces the probability of insecure

configurations being introduced in the field.

Usability – The ease with which users can operate a device safely and effectively. Security controls must be balanced with usability; overly complex authentication may lead users to circumvent security. Human-centered design is crucial for ensuring that security measures are adopted and maintained.

Regulatory Authority – The governmental body responsible for overseeing medical device compliance. Major authorities include the U.S. Food and Drug Administration (FDA), the European Medicines Agency (EMA) and its national competent authorities, Health Canada, and the Therapeutic Goods Administration (TGA) in Australia. Each authority has specific expectations for cybersecurity documentation and reporting.

Regulatory Submission – The package of documents submitted to a regulatory authority for market approval. Submissions typically include a technical file, design dossier, clinical evaluation, risk management file, and increasingly, a cybersecurity plan. The submission must demonstrate that the device meets safety, effectiveness, and security requirements.

Technical File – A collection of documents that provides evidence of a device's compliance with applicable standards. In the European Union, the technical file is part of the CE marking process. It contains design specifications, test results, labeling, and a risk management file that includes cybersecurity considerations.

Design Dossier – Similar to a technical file but used in the United Kingdom's regulatory framework post-Brexit. The design dossier contains detailed information about the device's design, manufacturing, and risk management, including cybersecurity controls.

CE Marking – The conformity mark indicating that a device complies with the EU Medical Device Regulation (MDR) or In Vitro Diagnostic Regulation (IVDR). The CE marking process requires a declaration of conformity, a technical file, and, for higher-risk devices, a conformity assessment by a Notified Body. Cybersecurity evidence must be part of the conformity assessment.

Notified Body – An independent organization designated by an EU member state to assess the conformity of certain medical devices. Notified Bodies review the technical file, conduct audits, and issue certificates. They evaluate the adequacy of the manufacturer's cybersecurity risk management and controls.

Class I, IIa, IIb, III – The classification system for medical devices based on risk. Class I devices are low risk, while Class III devices are high risk and typically life-supporting or invasive. Higher-risk classes require more rigorous regulatory scrutiny, including detailed cybersecurity assessments.

Medical Device Reporting (MDR) – The U.S. FDA's system for manufacturers to report adverse events and device malfunctions. Cybersecurity-related adverse events must be reported under this system, often as part of a medical device report (MDR) or a supplement to an existing report.

Software Validation – The process of confirming that software meets its intended purpose and regulatory requirements. Validation includes functional testing, performance testing, and security testing. For SaMD

and SiMD, validation must demonstrate that security controls do not adversely affect clinical functionality.

Verification – The process of confirming that a product or component meets its design specifications. Verification is distinct from validation; verification checks that the design is correctly implemented, while validation checks that the correct design was chosen.

Clinical Evaluation – The assessment of a device's clinical performance and safety based on data from clinical studies, literature, and post-market data. Cybersecurity considerations are increasingly part of clinical evaluation, especially when vulnerabilities could affect clinical outcomes.

Human Factors Engineering (HFE) – The discipline that studies how users interact with devices. HFE informs the design of security features to ensure they are usable and do not introduce new risks. For example, designing a password entry method that is both secure and easy for clinicians to use under time pressure.

Lifecycle Management – The ongoing process of maintaining a device from design through disposal. Lifecycle activities include updates, monitoring, incident response, and end-of-life planning. Effective lifecycle management ensures that cybersecurity controls remain effective throughout the device's operational life.

End-of-Life (EOL) – The point at which a manufacturer ceases to provide support, updates, or parts for a device. EOL planning must consider how devices will be safely decommissioned or transitioned to newer models, especially regarding data security and disposal of sensitive information.

Decommissioning – The process of removing a device from service and ensuring that all data is securely erased or transferred. Proper decommissioning prevents residual data from being accessed by unauthorized parties and is a regulatory requirement in many jurisdictions.

Incident Response Plan (IRP) – A documented set of procedures for detecting, containing, eradicating, and recovering from security incidents. The IRP should define roles, communication channels, escalation paths, and reporting obligations. Regulatory bodies often require evidence that an IRP is in place and tested.

Root Cause Analysis (RCA) – A systematic investigation to determine the underlying reasons for an incident or failure. In cybersecurity, RCA helps identify the origin of a breach, such as a misconfigured firewall or an unpatched vulnerability, and informs corrective actions.

Corrective Action – A step taken to eliminate the cause of a non-conformance or incident. Corrective actions may include software patches, configuration changes, or process improvements. Documentation of corrective actions is required for regulatory compliance.

Preventive Action – Measures taken to prevent the occurrence of a potential non-conformance. Examples include staff training on secure coding practices, supplier audits, and the implementation of automated vulnerability scanning.

Vulnerability Management System (VMS) – A tool or platform used to track, prioritize, and remediate vulnerabilities throughout the device's lifecycle. The VMS should integrate with risk management processes and generate reports for regulatory submissions.

Common Vulnerability Scoring System (CVSS) – A standardized method for rating the severity of vulnerabilities. CVSS scores help prioritize remediation efforts. For medical devices, a high CVSS score may trigger immediate action due to the potential impact on patient safety.

Secure Boot – A mechanism that ensures only authenticated firmware can be loaded during device startup. Secure boot prevents the execution of malicious code that could compromise the device before the operating system loads.

Trusted Platform Module (TPM) – A hardware component that provides cryptographic functions, such as key storage and secure boot verification. TPMs can be used to protect cryptographic keys and ensure integrity of firmware in medical devices.

Digital Signature – A cryptographic technique that verifies the authenticity and integrity of software or data. Firmware updates for a cardiac monitor are often signed digitally to assure that the update originates from the legitimate manufacturer and has not been tampered with.

Access Control List (ACL) – A set of rules that define which users or systems can access specific resources. ACLs are used in network devices, operating systems, and application layers to enforce authorization policies.

Firewall – A network security device that controls incoming and outgoing traffic based on predefined security rules. In a hospital, a firewall may separate the clinical device zone from the general IT network, limiting exposure to external threats.

Intrusion Detection System (IDS) – A system that monitors network or host activity for signs of malicious behavior. An IDS can alert administrators to suspicious traffic targeting a medical imaging device, enabling rapid response.

Intrusion Prevention System (IPS) – Similar to an IDS but capable of actively blocking detected threats. IPS devices can be configured to drop packets that match known attack signatures targeting device communication protocols.

Network Segmentation – The practice of dividing a network into isolated segments to limit the spread of attacks. Segmentation is a key control for protecting critical medical devices, as it reduces the attack surface and confines potential breaches.

Virtual Private Network (VPN) – An encrypted tunnel that provides secure remote access to a network. VPNs are often used by service engineers to connect to devices for maintenance while ensuring confidentiality and integrity of data in transit.

Patch Release Cycle – The schedule on which a manufacturer issues security updates. For medical devices, the patch release cycle must align with regulatory requirements for change control, validation, and documentation. Rapid patch cycles may be necessary for high-severity vulnerabilities.

Change Control – A formal process for managing modifications to a device's design, software, or documentation. Change control records the rationale, impact analysis, and validation activities associated with each change, including security patches.

Regulatory Gap Analysis – An assessment that compares an organization's current practices against regulatory requirements. In cybersecurity, a gap analysis may reveal missing controls, insufficient documentation, or inadequate incident response capabilities.

Compliance Audit – An independent review of an organization's adherence to regulatory standards. Audits may focus on documentation, process implementation, and evidence of security controls. Findings are reported to senior management and may trigger corrective actions.

Regulatory Guidance – Non-binding documents issued by authorities to clarify expectations. Notable guidance includes the FDA's "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" and the European Union's "MDR cybersecurity requirements." Guidance documents help manufacturers align their processes with regulatory expectations.

Premarket Submission – The dossier submitted before a device is marketed, such as an FDA 510(k) or a European CE technical file. For devices with significant cybersecurity risk, the submission must include a detailed cybersecurity risk management plan, threat analysis, and evidence of security testing.

510(k) Submission – The FDA pathway for demonstrating substantial equivalence to a legally marketed predicate device. Cybersecurity considerations are now part of the 510(k) review, especially for devices that incorporate software or network connectivity.

De Novo Classification – An FDA pathway for novel low-to-moderate risk devices that lack a predicate. The De Novo process requires a comprehensive risk analysis, including cyber risk, and may set a precedent for future devices.

Premarket Approval (PMA) – The FDA's most stringent review process for high-risk devices. A PMA submission must include extensive clinical data, risk management documentation, and a robust cybersecurity plan. The FDA may request additional security testing before approval.

European Union Medical Device Regulation (MDR) – The regulatory framework that replaced the Medical Device Directive (MDD) in May 2021. The MDR emphasizes a lifecycle approach, increased post-market surveillance, and explicit cybersecurity requirements.

In Vitro Diagnostic Regulation (IVDR) – The EU regulation governing in-vitro diagnostic devices. Like the MDR, the IVDR requires manufacturers to address cybersecurity risks for devices that process or transmit

patient data.

Health Canada Medical Device Regulations (CMDR) – The Canadian framework for medical device approval and post-market monitoring. Health Canada requires a risk management plan that includes cybersecurity considerations for devices with software components.

Therapeutic Goods Administration (TGA) – Australian Regulatory Framework – The TGA oversees medical device registration and compliance in Australia. The TGA expects manufacturers to demonstrate that cybersecurity risks are managed throughout the device lifecycle.

ISO 14971 – The international standard for medical device risk management. ISO 14971 provides a systematic process for identifying hazards, estimating risk, evaluating acceptability, and implementing controls. Cybersecurity hazards are treated as any other hazard under this standard.

ISO/IEC 27001 – The international standard for information security management systems (ISMS). While not specific to medical devices, ISO/IEC 27001 provides a framework for managing information security risks, which can be applied to device manufacturers and healthcare providers.

IEC 62304 – The standard for software lifecycle processes in medical devices. IEC 62304 defines development, maintenance, and risk management activities for software, including security testing and documentation of software updates.

IEC 80001 – The standard for the application of risk management to IT networks that incorporate medical devices. IEC 80001 addresses the integration of devices into hospital IT systems, emphasizing the need for coordinated risk management across the network.

ISO 13485 – The quality management system standard for medical device manufacturers. ISO 13485 requires documented procedures for design, production, and post-market activities, and it is often referenced in conjunction with cybersecurity controls.

Regulatory Submission Timeline – The schedule that outlines key milestones for preparing and delivering a submission. Timelines must accommodate risk assessments, security testing, documentation, and review cycles. Delays in cybersecurity testing can impact overall approval timelines.

Clinical Decision Support (CDS) – Software that provides clinicians with patient-specific recommendations. CDS systems that operate on medical devices must be validated for both clinical accuracy and cybersecurity resilience, as compromised recommendations could lead to patient harm.

Interoperability – The ability of devices and systems to exchange and interpret data reliably. Interoperability standards such as HL7, FHIR, and DICOM must be implemented securely to prevent data tampering or unauthorized access.

Health Level Seven (HL7) – A set of standards for exchanging health information. Secure implementation of

HL7 interfaces is essential for protecting patient data and ensuring that malicious messages cannot disrupt device operation.

Fast Healthcare Interoperability Resources (FHIR) – A modern HL7 standard that uses RESTful APIs. FHIR APIs must be protected with authentication, authorization, and encryption to prevent unauthorized data access or injection attacks.

Digital Imaging and Communications in Medicine (DICOM) – The standard for handling, storing, and transmitting medical images. DICOM communication channels must be secured to prevent image tampering, unauthorized viewing, or ransomware attacks on imaging servers.

Radio Frequency Identification (RFID) – A technology used for tracking devices and supplies. RFID can be a target for spoofing attacks; therefore, authentication mechanisms should be implemented to verify tag authenticity.

Bluetooth Low Energy (BLE) – A wireless protocol commonly used in wearable medical devices. BLE security includes pairing mechanisms, encryption, and device whitelisting to protect against eavesdropping and unauthorized control.

Wi-Fi Protected Access (WPA3) – The latest Wi-Fi security protocol, providing stronger encryption and protection against brute-force attacks. Devices that support Wi-Fi connectivity should implement WPA3 where feasible.

Secure Firmware Update – The process of delivering firmware patches in a manner that ensures authenticity and integrity. Secure update mechanisms typically involve digital signatures, encrypted transmission, and verification before installation.

Rollback Protection – A control that prevents an attacker from installing an older, vulnerable version of firmware. Rollback protection can be enforced through version checks and secure boot validation.

Zero-Trust Architecture (ZTA) – A security model that assumes no implicit trust for any user or device, regardless of location. Implementing ZTA for medical devices involves continuous verification, micro-segmentation, and strict access controls.

Security Incident Metrics – Quantitative measures used to assess the effectiveness of security programs. Metrics may include mean time to detect (MTTD), mean time to respond (MTTR), number of incidents per device, and percentage of patches applied within a defined timeframe.

Mean Time to Detect (MTTD) – The average time taken to identify a security incident after it occurs. Reducing MTTD is critical for limiting the impact of attacks on medical devices.

Mean Time to Respond (MTTR) – The average time required to contain and remediate an incident. Efficient MTTR helps restore device functionality quickly, minimizing disruption to patient care.

Security Patch Deployment – The act of distributing and installing security updates across a fleet of devices. Deployment must be coordinated with clinical schedules to avoid interfering with patient treatment.

Device Hardening – The process of strengthening a device's configuration to reduce vulnerabilities. Hardening may involve disabling unused services, applying secure default settings, and enforcing strong authentication.

Configuration Management – The systematic handling of device settings throughout the lifecycle. Configuration management tools track changes, enforce policies, and ensure that devices remain in a secure state.

Incident Command System (ICS) – A standardized approach for managing emergency response, including cybersecurity incidents. The ICS defines roles such as Incident Commander, Operations Section Chief, and Public Information Officer, facilitating coordinated actions.

Public Disclosure – The act of publishing vulnerability information to the broader community. Manufacturers must balance transparency with the risk of providing attackers with useful details; coordinated disclosure processes help manage this tension.

Coordinated Vulnerability Disclosure (CVD) – A structured process where researchers, manufacturers, and authorities work together to address vulnerabilities before public release. CVD promotes responsible handling of security flaws and aligns with regulatory expectations for timely remediation.

Cybersecurity Maturity Model – A framework that assesses an organization's level of cybersecurity capability. Models such as the NIST Cybersecurity Framework (CSF) can be adapted for medical device manufacturers to benchmark progress.

National Institute of Standards and Technology (NIST) Cybersecurity Framework – A set of standards, guidelines, and best practices for managing cybersecurity risk. The NIST CSF's five functions—Identify, Protect, Detect, Respond, Recover—map well to medical device risk management processes.

Identify Function – The activity of developing an understanding of the organizational environment to manage cybersecurity risk. For medical devices, this includes asset inventory, threat identification, and risk assessment.

Protect Function – The implementation of safeguards to limit or contain the impact of a potential cybersecurity event. Controls include access management, data encryption, and secure development practices.

Detect Function – The capability to identify the occurrence of a cybersecurity event. Detection mechanisms may involve monitoring logs, intrusion detection, and anomaly detection algorithms.

Respond Function – The actions taken to contain, mitigate, and recover from a cybersecurity incident.

Response activities include incident handling, communications, and forensic analysis.

Recover Function – The processes for restoring normal operations and improving resilience after an incident. Recovery may involve patch deployment, system restoration, and lessons-learned activities.

Supply Chain Security Assurance (SCSA) – The verification that suppliers meet defined security requirements. SCSA may involve supplier questionnaires, audits, and contractual security clauses.

Trusted Supplier Program – A program that establishes criteria for evaluating and approving suppliers based on security posture, certifications, and past performance. Participation in a trusted supplier program can reduce supply chain risk.

Regulatory Inspection – An on-site review conducted by a regulatory authority to verify compliance. Inspectors may examine documentation, test equipment, and interview personnel to assess the adequacy of cybersecurity controls.

Design Transfer – The process of moving a device design from development to manufacturing. Design transfer documentation must include security specifications, testing results, and configuration settings to ensure that security is maintained during production.

Manufacturing Process Validation (MPV) – The demonstration that manufacturing processes consistently produce devices meeting specifications. MPV includes validation of software loading, hardware assembly, and security control implementation.

Device Identification (UDI) – A unique identifier assigned to each medical device model and, in some cases, each individual unit. The UDI system improves traceability, enabling faster recall of devices affected by a cybersecurity vulnerability.

Recall – The removal of a device from the market due to safety concerns. Cybersecurity-related recalls may be triggered by a critical vulnerability that cannot be mitigated through a patch.

Field Safety Notice (FSN) – A communication from a manufacturer to users about a safety issue, often providing instructions for temporary mitigation. FSNs are commonly used when a rapid patch is not yet available.

Software Bill of Materials (SBOM) – A detailed inventory of all software components, libraries, and dependencies used in a device. An SBOM helps identify vulnerable third-party components and supports compliance with supply chain security requirements.

Third-Party Component – Any software or hardware element sourced from an external supplier. Common third-party components include operating system kernels, cryptographic libraries, and sensor modules. Each component must be assessed for security risks.

Open-Source Software (OSS) – Software with publicly available source code. OSS can accelerate development but also introduces risks if vulnerabilities are not promptly addressed. Manufacturers should track OSS usage and apply security patches as they become available.

Code Review – The systematic examination of source code to detect security flaws, logic errors, and compliance issues. Peer reviews, automated static analysis, and manual inspection all contribute to a thorough code review process.

Secure Coding Standards – Guidelines that define best practices for writing safe software. Examples include the CERT C Secure Coding Standard and the OWASP Secure Coding Practices. Adhering to these standards reduces the likelihood of introducing vulnerabilities.

Patch Validation – The process of testing a security patch to ensure it does not introduce new defects or compromise device functionality. Validation may involve regression testing, performance testing, and safety verification.

Regression Testing – Testing that confirms existing functionality continues to work after changes such as a security patch. Regression testing is essential for maintaining device reliability and compliance.

Performance Testing – The evaluation of a device's operational characteristics, such as response time or throughput, after implementing security controls. Performance testing ensures that security measures do not degrade clinical performance.

Safety Verification – The confirmation that safety-related functions remain effective after security updates. For instance, verifying that an alarm system still triggers correctly after a firmware patch.

Regulatory Documentation – The collection of records required to demonstrate compliance. Documentation includes risk management files, test reports, validation plans, and incident logs. Maintaining accurate documentation is critical for successful audits.

Electronic Health Record (EHR) Integration – The connection between medical devices and patient record systems. Secure integration requires authentication, encryption, and audit trails to protect patient data and ensure data integrity.

Audit Trail – A chronological record of system activities, such as user actions, configuration changes, and data access. Audit trails support forensic investigations and must be protected from tampering.

Data Integrity – The assurance that data is accurate, complete, and unaltered. In medical devices, integrity checks may involve checksums, digital signatures, and redundancy mechanisms.

Data Confidentiality – The protection of patient information from unauthorized disclosure. Confidentiality controls include encryption, access restrictions, and secure storage.

Data Availability – The guarantee that data and services are accessible when needed. Redundant architectures, failover mechanisms, and denial-of-service mitigation strategies support availability.

Denial-of-Service (DoS) Attack – An attempt to make a device or service unavailable by overwhelming it with traffic or exploiting resource-exhaustion vulnerabilities. DoS attacks on networked infusion pumps could delay medication delivery, posing a risk to patients.

Ransomware – Malware that encrypts data and demands payment for decryption. A ransomware infection of a radiology server could block access to imaging studies, delaying diagnosis and treatment.

Malware – Software designed to disrupt, damage, or gain unauthorized access to computer systems. Malware targeting medical devices may aim to alter device settings, exfiltrate data, or create backdoors.

Backdoor – An undocumented method of accessing a system, often left by developers for troubleshooting. Backdoors are high-risk security flaws because they can be exploited by attackers to gain control of a device.

Supply Chain Attack – An intrusion that targets a component or software supplier to compromise downstream products. The 2020 SolarWinds incident illustrates how a compromised update can affect thousands of organizations, including healthcare providers.

Zero-Day Vulnerability – A flaw that is unknown to the vendor and has no available patch. Zero-day exploits are particularly dangerous for medical devices because they may be used before any mitigations can be deployed.

Threat Intelligence – Information about emerging threats, attackers, tactics, techniques, and procedures (TTPs). Threat intelligence feeds help manufacturers anticipate new attack vectors and prioritize defensive measures.

Security Information and Event Management (SIEM) – A platform that aggregates, correlates, and analyzes log data from multiple sources to detect security incidents. SIEM solutions can be configured to monitor medical device logs for anomalous behavior.

Log Management – The collection, storage, and analysis of log data. Proper log management ensures that evidence is available for incident investigation and compliance reporting.

Forensic Analysis – The systematic examination of digital evidence to reconstruct the events of a security incident. Forensic analysis may involve imaging a device’s storage, analyzing network traffic, and identifying malicious code.

Chain of Custody – The documentation of evidence handling from collection to presentation, preserving its integrity. Maintaining a clear chain of custody is essential for legal and regulatory investigations.

Legal Hold – A directive to preserve all relevant data and documents in anticipation of litigation. A legal hold may be triggered by a cybersecurity breach that results in patient injury.

Regulatory Enforcement Action – Actions taken by authorities to compel compliance, such as fines, product recalls, or suspension of market authorization. Failure to adequately address cybersecurity risks can lead to enforcement actions.

Compliance Officer – The individual responsible for ensuring that the organization meets regulatory requirements. The compliance officer coordinates with engineering, quality, and legal teams to address cybersecurity obligations.

Quality Management System (QMS) – A structured system of processes and procedures that ensure product quality. The QMS must integrate cybersecurity controls to meet standards such as ISO 13485.

Documentation Control – The process of managing documents to ensure that the latest versions are used and obsolete documents are archived. Effective control prevents the use of outdated security procedures.

Training and Awareness – Educational programs that inform staff about security policies, safe practices, and incident reporting.