Certified Specialist Programme in Medical Device Cybersecurity

Regulatory Framework for Medical Devices

A – Adverse Event: Any undesirable experience associated with the use of a medical device, whether or not it is caused by the device. Related terms: Incident, Harm, Patient Safety. Example: A pacemaker delivering inappropriate shocks. Practical application: Reporting to the national competent authority within the stipulated time frame. Challenge: Distinguishing device-related events from underlying disease.

AE – Adverse Event Report: A documented submission describing an adverse event. Related terms: MAUDE, Vigilance. Explanation: Must include device identification, patient outcome, and root cause analysis. Example: Submission of a malfunction report for an insulin pump. Challenge: Ensuring completeness under time constraints.

AF – Authorization for Use: Formal permission granted by a regulatory body to market a device. Related terms: CE Mark, FDA 510(k). Explanation: Confirms compliance with applicable safety and performance standards. Example: A hospital receiving an AF for a new surgical robot. Challenge: Maintaining the authorization after post-market changes.

AI – Artificial Intelligence: Computer systems that perform tasks requiring human intelligence. Related terms: Machine Learning, Neural Network. Explanation: In medical devices, AI can analyze imaging or monitor physiological data. Example: AI-driven ECG interpretation. Challenge: Ensuring algorithm transparency and managing data bias.

AL – Alert Level: A predefined severity classification used to prioritize response to a cybersecurity incident. Related terms: Incident Severity, Risk Rating. Explanation: Levels range from low (informational) to critical (system compromise). Example: An alert level “high” for ransomware detection on a ventilator network. Challenge: Aligning alert levels across diverse device types.

AM – Asset Management: Process of identifying, cataloguing, and maintaining an inventory of devices and their components. Related terms: Configuration Management, CMDB. Explanation: Enables traceability of hardware and software versions. Example: Maintaining a database of all infusion pumps in a facility. Challenge: Keeping inventory current amid rapid device turnover.

AP – Audit Protocol: Structured method for reviewing compliance with regulatory and security requirements. Related terms: Internal Audit, Inspection. Explanation: Includes checklists, evidence collection, and corrective action tracking. Example: Conducting an audit of encryption practices on wireless telemetry devices. Challenge: Balancing audit depth with operational disruption.

AS – Assurance Statement: Document affirming that a device meets specified security controls. Related terms: Security Assurance, Compliance Report. Explanation: Often required for high-risk devices before market entry. Example: An assurance statement that a cardiac monitor complies with IEC 62443. Challenge: Providing evidence for evolving threats.

B – Baseline Configuration: The approved set of hardware, software, and settings that define a secure operating state. Related terms: Hardened Image, Reference Configuration. Explanation: Used as a starting point for security monitoring. Example: Deploying a baseline OS image on all bedside monitors. Challenge: Updating the baseline without introducing drift.

BIA – Business Impact Analysis: Assessment of the potential consequences of a disruption to device services. Related terms: Risk Assessment, Continuity Planning. Explanation: Identifies critical functions and recovery priorities. Example: Analyzing the impact of network outage on insulin delivery systems. Challenge: Quantifying indirect patient harm.

C – Classification: Determination of device risk class based on intended use and potential harm. Related terms: Class I, Class II, Class III. Explanation: Drives regulatory pathway and post-market obligations. Example: Class IIa for a diagnostic ultrasound probe. Challenge: Re-classification when software updates add new functions.

CE – Conformité Européenne: Symbol indicating that a device complies with EU safety, health, and environmental requirements. Related terms: Notified Body, EU MDR. Explanation: Mandatory for market access in the European Economic Area. Example: A wearable glucose monitor bearing the CE mark. Challenge: Maintaining conformity after a cybersecurity patch.

CM – Change Management: Formal process for proposing, evaluating, approving, and implementing modifications to a device. Related terms: Configuration Control, Versioning. Explanation: Ensures that changes do not degrade safety or security. Example: Updating firmware on a defibrillator. Challenge: Coordinating changes across multiple stakeholders.

CMR – Clinical Monitoring Report: Documentation of ongoing clinical performance data collected post-market. Related terms: PMS, Post-Market Surveillance. Explanation: Provides evidence of continued safety and efficacy. Example: Quarterly CMR for a smart inhaler. Challenge: Integrating cybersecurity metrics into clinical data.

CPS – Cyber-Physical System: Integration of computation, networking, and physical processes. Related terms: IoT, Embedded System. Explanation: In medical devices, CPS enables real-time monitoring and actuation. Example: A robotic surgery platform that receives commands over a network. Challenge: Protecting the feedback loop from malicious manipulation.

CS – Cybersecurity Standard: Prescribed set of security controls for medical devices. Related terms: IEC 62443, FDA Guidance. Explanation: Provides baseline requirements for confidentiality, integrity, and availability. Example: Implementing secure boot as required by a CS. Challenge: Mapping generic standards to device-specific risk profiles.

D – Device Identification: Unique labeling that distinguishes a specific device model, version, and serial number. Related terms: UDI, Lot Number. Explanation: Facilitates traceability throughout the product lifecycle. Example: Scanning the barcode on a surgical stapler to retrieve its UDI. Challenge: Managing legacy devices lacking digital identifiers.

DCA – Device Cybersecurity Assessment: Systematic evaluation of a device's security posture. Related terms: Penetration Test, Vulnerability Scan. Explanation: Includes threat modeling, code review, and resilience testing. Example: Conducting a DCA on an MRI system's network interfaces. Challenge: Balancing thoroughness with manufacturer cooperation.

DH – Data Handling: Processes for collection, storage, transmission, and disposal of device data. Related terms: Data Encryption, Data Retention. Explanation: Must comply with privacy regulations and maintain integrity. Example: Encrypting patient telemetry before sending to the cloud. Challenge: Ensuring secure data lifecycle across multiple jurisdictions.

DM – Device Manufacturer: Entity responsible for design, production, and post-market activities of a medical device. Related terms: OEM, Supplier. Explanation: Holds primary accountability for regulatory compliance. Example: A company producing implantable cardiac devices. Challenge: Coordinating cybersecurity responsibilities across a global supply chain.

DR – Design Review: Formal evaluation of device design to verify that requirements are met. Related terms: Verification, Validation. Explanation: Includes security considerations such as threat analysis. Example: Reviewing the encryption algorithm selection during the design phase of a pacemaker. Challenge: Incorporating security early without inflating development timelines.

E – Encryption: Process of converting data into a coded form to prevent unauthorized access. Related terms: Symmetric Key, Asymmetric Key, TLS. Explanation: Essential for protecting data at rest and in transit. Example: Using AES-256 to encrypt stored imaging files. Challenge: Managing key lifecycle and performance constraints on low-power devices.

EUA – Emergency Use Authorization: Temporary regulatory permission to use a device during a public health emergency. Related terms: EUA, Compassionate Use. Explanation: Allows expedited deployment with limited data. Example: Authorization of a ventilator firmware update during a pandemic surge. Challenge: Ensuring post-EUA security monitoring.

F – Firmware: Low-level software that controls hardware functions. Related terms: Bootloader, Update, Patch. Explanation: Often the target of cyber attacks due to privileged access. Example: Updating the firmware of an insulin pump to fix a buffer overflow. Challenge: Providing secure, authenticated update mechanisms.

FA – Failure Analysis: Investigation of the root cause of a device malfunction. Related terms: RCA, Fault Tree. Explanation: Determines whether the failure is safety-related or security-related. Example: Analyzing a sudden loss of power in a bedside monitor. Challenge: Distinguishing accidental failures from deliberate sabotage.

G – Gap Analysis: Comparison of current security practices against required standards. Related terms: Benchmarking, Compliance Gap. Explanation: Identifies deficiencies and prioritizes remediation. Example: Conducting a gap analysis of a hospital's network segmentation against IEC 62443. Challenge: Aligning multiple regulatory expectations.

H – Hazard Analysis: Process of identifying potential sources of harm associated with a device. Related terms: FMEA, Fault Tree Analysis. Explanation: Forms the basis for risk management. Example: Hazard analysis of a wireless blood pressure cuff identifying radio interference as a risk. Challenge: Extending traditional hazard analysis to include cyber threats.

I – Incident Response: Structured approach to detect, contain, eradicate, and recover from a security event. Related terms: IR Plan, SOC, Forensics. Explanation: Requires defined roles, communication channels, and escalation paths. Example: Activating the IR plan after detection of unauthorized access to a cardiac monitor. Challenge: Coordinating response across clinical, IT, and regulatory teams.

IEC – International Electrotechnical Commission: Global organization that publishes standards for electrical and electronic devices. Related terms: IEC 60601, IEC 62443. Explanation: Provides safety (IEC 60601) and security (IEC 62443) frameworks. Example: Compliance with IEC 60601-1 for electrical safety of a defibrillator. Challenge: Interpreting standards that are technology-agnostic for modern cyber-enabled devices.

ISO – International Organization for Standardization: Body that develops international standards across many domains. Related terms: ISO 14971, ISO 27001. Explanation: ISO 14971 governs risk management for medical devices; ISO 27001 addresses information security management. Example: Using ISO 14971 to assess risks of a software-only glucose monitor. Challenge: Mapping ISO 27001 controls to device-level security requirements.

J – Joint Commission: U.S. Organization that accredits health care organizations and sets safety standards. Related terms: NPSG, Sentinel Event. Explanation: Requires institutions to manage device security as part of overall patient safety. Example: Reporting a sentinel event caused by a compromised infusion pump. Challenge: Aligning Joint Commission expectations with device-specific regulations.

K – Key Management: Procedures for generating, distributing, storing, rotating, and revoking cryptographic keys. Related terms: PKI, HSM. Explanation: Critical for maintaining encryption effectiveness. Example: Using a hardware security module to store device private keys. Challenge: Implementing automated key rotation without disrupting clinical workflows.

L – Lifecycle Management: Oversight of a device from conception through disposal. Related terms: PLM, End-of-Life (EOL). Explanation: Includes planning for security updates and de-commissioning. Example: Scheduling firmware updates for a networked infusion pump throughout its five-year service life. Challenge: Ensuring security patches are delivered before devices reach EOL.

M – MDR – Medical Device Regulation: European Union regulation (EU 2017/745) governing the safety and performance of medical devices. Related terms: EU MDR, Notified Body. Explanation: Introduces stricter post-market surveillance and traceability requirements. Example: Updating the technical file of a Class IIb device to meet MDR. Challenge: Aligning existing CE-Marked devices with new MDR obligations.

N – Notified Body: Independent organization designated by an EU member state to assess conformity of medical devices. Related terms: NB, CE Mark. Explanation: Conducts audits, reviews technical documentation, and issues certificates. Example: A Notified Body reviewing the cybersecurity risk

assessment for a new robotic catheter system. Challenge: Coordinating timelines between manufacturer and NB for rapid market entry.

O – OEM – Original Equipment Manufacturer: Company that designs and builds a medical device, often integrating third-party components. Related terms: Supplier, Sub-contractor. Explanation: Holds ultimate responsibility for device compliance. Example: An OEM incorporating a third-party sensor module into a wearable monitor. Challenge: Managing security of embedded third-party software.

P – Post-Market Surveillance (PMS): Ongoing process of collecting and analyzing data on device performance after it is on the market. Related terms: CMR, Vigilance, REMS. Explanation: Includes safety, efficacy, and cybersecurity monitoring. Example: Quarterly PMS reports documenting vulnerability disclosures for a remote monitoring platform. Challenge: Integrating cyber incident data with clinical outcomes.

Q – Quality Management System (QMS): Organized set of procedures and processes to ensure product quality and regulatory compliance. Related terms: ISO 13485, CAPA. Explanation: QMS must incorporate security controls as part of risk management. Example: Documenting a corrective action for a discovered firmware vulnerability within the QMS. Challenge: Extending traditional QMS documentation to cover cyber-related CAPA.

R – Risk Management: Systematic identification, evaluation, control, and monitoring of risks throughout the device lifecycle. Related terms: ISO 14971, Hazard Analysis. Explanation: Must address both safety and security threats. Example: Performing a risk assessment that includes potential ransomware attacks on a networked infusion pump. Challenge: Quantifying likelihood of sophisticated cyber threats.

S – Software Bill of Materials (SBOM): Detailed inventory of all software components, libraries, and dependencies in a device. Related terms: Dependency Management, Open Source. Explanation: Enables tracking of known vulnerabilities. Example: Publishing an SBOM for a cardiac telemetry system that lists the OpenSSL version used. Challenge: Maintaining accurate SBOMs as firmware evolves.

T – Threat Modeling: Structured approach to identify potential attackers, attack vectors, and assets. Related terms: STRIDE, PASTA. Explanation: Informs security design and mitigation strategies. Example: Applying STRIDE to a wireless infusion pump to assess spoofing and tampering risks. Challenge: Keeping the model current with emerging threat intelligence.

U – UDI – Unique Device Identifier: Global system for device identification that facilitates traceability and recall. Related terms: GS1, HIBCC. Explanation: Consists of a device identifier (DI) and production identifier (PI). Example: Scanning the UDI barcode on a sterile surgical instrument to retrieve batch information. Challenge: Integrating UDI data into cybersecurity incident logs.

V – Vulnerability Disclosure: Process by which security researchers report discovered weaknesses to the manufacturer. Related terms: CVE, Bug Bounty, Responsible Disclosure. Explanation: Enables timely remediation before exploitation. Example: A researcher submits a CVE for a buffer overflow in a pacemaker's communication module. Challenge: Coordinating disclosure timelines with regulatory reporting obligations.

W – WHO – World Health Organization: International body that issues guidance on health technologies, including device safety. Related terms: GHTF, IMDRF. Explanation: Publishes global standards and recommendations that influence national regulations. Example: WHO's guidance on digital health security influencing national policy. Challenge: Translating broad WHO recommendations into device-specific controls.

X – eXternal Interface: Any point where a device connects to external systems, networks, or users. Related terms: API, Port, Connector. Explanation: Represents a potential attack surface. Example: A Bluetooth interface on a glucose monitor used for data transfer. Challenge: Securing interfaces without compromising usability.

Y – Y2K-Like Legacy Issue: Problems arising from outdated software architectures that cannot support modern security controls. Related terms: Legacy System, Technical Debt. Explanation: Legacy devices may lack patchability or encryption. Example: An older bedside monitor that runs an unsupported operating system. Challenge: Mitigating risk while awaiting device replacement.

Z – Zero-Trust Architecture: Security model that assumes no implicit trust, even within the perimeter. Related terms: Micro-segmentation, Identity-Based Access. Explanation: Applies strict verification for every device interaction. Example: Enforcing mutual TLS between a central monitoring station and each bedside device. Challenge: Implementing zero-trust in environments with legacy equipment and limited compute resources.