digicert®

FDA Cybersecurity Premarket Submissions: A Compliance Guide for Medical Device Manufacturers

Understand FDA expectations and build secure-by-design devices that earn trust.

WHITE PAPER

Understand FDA expectations and build secure-by-design devices that earn trust.

1. Introduction

The U.S. Food and Drug Administration (FDA) now considers cybersecurity a critical element of medical device safety and effectiveness. As connected medical devices become integral to patient care, the risk of cyber incidents affecting hospitals, patients, and healthcare infrastructure has grown significantly.

Historically, cybersecurity was treated as an operational or post-market consideration. Today, FDA guidance makes it clear:

- Cybersecurity is a requirement for market access
- Premarket submissions must demonstrate compliance with a myriad of requirements, including secure-by-design architecture
- Manufacturers must manage vulnerabilities and maintain device trust throughout the lifecycle

Why This Matters

Connected medical devices—from infusion pumps and diagnostic imaging systems to wearable monitors—are part of a complex digital healthcare ecosystem. Vulnerabilities in these devices can:

- Put patients at risk if device functionality is disrupted
- Expose hospitals to cyberattacks and compliance violations
- Force regulatory actions such as market withdrawals or costly redesigns

FDA's updated premarket cybersecurity guidance reflects a fundamental shift: security is safety. Manufacturers must now prove that cybersecurity controls are in place from the start and can be maintained for the entire product lifecycle.

About This Guide

This guide is designed to help medical device manufacturers understand and align with FDA premarket cybersecurity expectations. It provides:

1. An overview of FDA cybersecurity guidance and its impact on medical device submissions
2. Detailed security control recommendations drawn from FDA guidance, including the tables your regulatory teams need for submissions
3. Practical takeaways for OEMs to integrate cybersecurity in design, development, and postmarket processes

Manufacturers who use this guide will be better prepared to:

- Build secure-by-design devices
- Document and justify security controls in premarket submissions
- Accelerate regulatory review and reduce the risk of delays or postmarket exposure

2. FDA Cybersecurity Guidance Overview

The U.S. Food and Drug Administration has made it clear that cybersecurity is patient safety. In recent updates to its premarket cybersecurity guidance for medical devices, the FDA outlines expectations for manufacturers to demonstrate secure-by-design architecture, transparent documentation, and lifecycle vulnerability management as part of the device approval process.

Manufacturers must now treat cybersecurity as a core design requirement, not an afterthought. Premarket submissions that fail to adequately address cybersecurity policies and practices risk encountering delays, additional information requests (AI letters), or outright refusal to accept (RTA).

2.1 FDA Objectives

FDA's cybersecurity guidance is designed to ensure that medical devices:

1. Protect patient safety and clinical functionality
    - Devices must remain safe and effective even under cyberattack scenarios.
2. Reduce risks to healthcare infrastructure
    - Compromised devices should not propagate threats to hospital networks or cloud ecosystems.
3. Enable transparency and traceability
    - Submissions must include evidence, such as SBOMs, signed firmware, and documented patch processes.
4. Support postmarket resilience
    - Manufacturers are expected to monitor, disclose, and remediate vulnerabilities for the life of the device

2.2 Scope of Devices and Submissions

The FDA's cybersecurity guidance applies broadly to medical devices with digital components, including:

- Connected and network-enabled devices
    - Infusion pumps, patient monitors, implantable devices with telemetry
- Standalone software and SaMD (Software as a Medical Device)
    - Applications that process or transmit patient data
- Systems with cloud or wireless connectivity
    - Devices that interface with hospital IT networks or external cloud services

Both new device submissions and significant updates to previously approved devices must now include cybersecurity documentation that demonstrates security measures are integrated into design, development, and lifecycle management.

2.3 Core Premarket Expectations

In its guidance, the FDA emphasizes three core areas of focus for cybersecurity in premarket submissions:

1. Secure-by-Design Architecture
    - Devices must be built with security in mind from the earliest stages of development.
    - Attack surfaces should be minimized, and critical functions must be resilient to cyber incidents.
2. Comprehensive Documentation
    - Submissions must include:
        - Software Bill of Materials (SBOM) in machine-readable format
        - Signed firmware and update processes
        - Risk assessments and threat modeling evidence
3. Lifecycle and Vulnerability Management
    - Manufacturers must provide plans for:
        - Vulnerability monitoring and coordinated disclosure
        - Secure and timely updates (including over-the-air where applicable)
        - Incident containment and recovery measures

2.4 FDA Review Perspective

FDA reviewers will evaluate premarket submissions to ensure that:

- Cybersecurity is treated as part of device safety
- Risks are mitigated through design, not just documentation
- Evidence demonstrates the ability to maintain security over time

Failure to meet these expectations can lead to additional information requests (AI letters), delayed approvals, or post-market obligations that impact time-to-market and brand trust.

3. Security Control Categories and Recommendations

The FDA's Cybersecurity Premarket Guidance requires medical device manufacturers to demonstrate that connected devices are secure, resilient, and maintainable throughout their lifecycle.

In this section, we break down the four key security control categories that OEMs must address in their premarket submissions:

1. Design and Development Controls – Security built in from the start
2. Testing and Documentation Requirements – Proving security through evidence
3. Secure Update and Vulnerability Management – Responding to emerging threats
4. Post-Market and Lifecycle Security – Maintaining long-term trust and safety

Each subsection explains:

- Why the control matters for patient safety and regulatory compliance
- Key OEM practices and pitfalls for building a defensible FDA submission
- How FDA reviewers evaluate security readiness

The full set of 50 FDA recommendations and DigiCert's compliance support can be found in Appendix 1.

3.1 Design and Development Controls

Building security into a device during design is the foundation of regulatory compliance and patient safety. FDA's premarket guidance expects devices to be secure-by-design, which requires that OEMs:

1. Minimize attack surfaces by disabling unused interfaces and services
2. Authenticate and authorize all users, services, and connected systems
3. Ensure code and data integrity with secure boot and cryptographic enforcement
4. Protect sensitive data through FIPS-validated cryptography

Why This Matters

Secure-by-design devices have faster approvals, lower lifecycle risk, and higher trust with healthcare customers.

See Appendix 1 – Design and Development Controls (Recommendations 1–15) for the complete list and DigiCert support details.

3.2 Testing and Documentation Requirements

Even the most secure medical device will face regulatory scrutiny if security measures are not clearly documented, verified, and supported with evidence.

FDA reviewers are no longer accepting vague claims like "security features implemented" without traceable, testing-backed proof that the device is safe and resilient in real world conditions.

Strong testing and documentation practices give OEMs a regulatory advantage, reducing AI (Additional Information) requests and speeding time- to- market.

Building security into a device during design is the foundation of regulatory compliance and patient safety.

Why Testing and Documentation Matter

Cybersecurity is directly tied to patient safety. A device that can be compromised puts both patients and healthcare networks at risk. FDA reviewers want to see that:

1. The device has been thoroughly tested against realistic threats
2. The OEM can demonstrate its security posture with evidence
3. The submission connects each risk to a specific mitigation and test result

When documentation is incomplete, vague, or poorly mapped to risks, reviewers are forced to request additional information—causing delays that can last weeks or months.

Key Testing and Documentation Practices for OEMs

1. Comprehensive Software Bill of Materials (SBOMs)
    - Provide an SBOM for every release in machine-readable formats like SPDX or CycloneDX.
    - Include all opensource and third-party components, as FDA expects visibility into potential vulnerabilities.
    - Maintain version history and dependency chains, which support vulnerability management and post-market remediation.
2. Evidence Driven Security Verification
    - Conduct and submit results from:
        - Penetration testing and fuzzing
        - Static and dynamic code analysis
        - Cryptographic module verification and functional tests
    - FDA expects test evidence to directly support the security claims made in the submission.
3. Traceable Risk-to-Mitigation Mapping
    - Security documentation should connect each identified risk to its mitigation.
        - Example:
            1. Risk: Unauthorized firmware modification
            2. Mitigation: Signed firmware with secure boot
            3. Evidence: Signature validation test results included in submission
4. Submission Ready Test Artifacts
    - Include executive summaries and interpretable results—raw logs alone are insufficient.
    - A strong submission bundles SBOMs, risk assessments, test plans, results, and mitigation evidence into an organized package.

OEM Insights and Pitfalls

- **Common Pitfall:** Submitting a raw SBOM without clear connections to risk mitigations or vulnerability scans.
- **Pro Tip:** FDA prefers submissions where security evidence is curated and consumable—think of it as telling a security story.
- **High Performing OEMs:** Maintain an internal "regulatory package" that ties together SBOMs, test results, and design artifacts, ensuring readiness for both premarket review and post-market audits.

For the complete list of Testing and Documentation recommendations and how DigiCert solutions support each requirement, see Appendix 1 – Recommendations 16–25.

3.3 Secure Update and Vulnerability Management

A connected medical device is never truly finished.

Even after FDA clearance, the device's cybersecurity posture must evolve with emerging threats. Vulnerabilities in third-party libraries, cryptographic algorithms, or wireless protocols can expose devices—and patients—to significant risk if left unaddressed.

FDA's Cybersecurity Premarket Guidance requires OEMs to demonstrate the ability to patch and update devices securely, and to manage vulnerabilities across the full lifecycle.

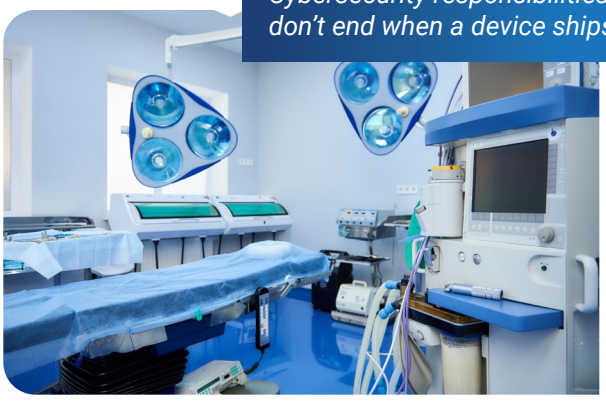
Why Secure Update Capabilities Are Critical

- Cyber threats evolve faster than hardware refresh cycles.
- A device may be in the field for 7–10 years, during which new vulnerabilities will inevitably appear.
- Patient safety depends on timely updates.
- An exploited vulnerability could lead to incorrect therapy, service interruptions, or network compromise.
- Regulatory compliance now requires proactive lifecycle management.
- OEMs must prove they can issue security updates before vulnerabilities become patient safety events.

Key Practices for OEMs

1. Cryptographically Signed Updates
    - Every update—whether delivered OTA (over-the-air) or via physical media—must be signed and validated before execution.
    - FDA expects evidence of signature verification in the premarket submission.
    - **Pro Tip:** Pair signed updates with secure boot to create a chain of trust from manufacturing- to- field deployment.
2. Anti-Rollback and Anti-Replay Protections
    - Devices must reject outdated or tampered updates to prevent attackers from reinstalling vulnerable firmware.
    - Demonstrate version control and validation logic as part of your cybersecurity documentation.
3. Vulnerability Monitoring and Patch Management
    - Establish a formal process for monitoring CVEs and security advisories affecting your SBOM components.
    - OEMs should define remediation timelines in line with FDA expectations (often 30–60 days for critical vulnerabilities).
    - **Common Pitfall:** Lacking an actionable plan for dependencies in third-party libraries or opensource code.
4. Update Delivery Strategy
    - Support secure, efficient OTA updates where feasible to accelerate remediation.
    - Include mechanisms for fleetwide update tracking to prove to FDA—and your customers—that devices are maintained securely.

Cybersecurity responsibilities don't end when a device ships.



OEM Insights and Pitfalls

- Weak submissions often describe "update capability" but fail to demonstrate cryptographic validation or rollback protection.
- Strong submissions include:
    - Signed firmware validation logic
    - Version management plans
    - Patch latency commitments supported by process documentation
- **Pro Tip:** Hospitals increasingly require proof of a vendor's secure update and vulnerability management process as part of purchasing decisions.

For the complete list of Secure Update and Vulnerability Management recommendations and how DigiCert solutions support each requirement, see Appendix 1 – Recommendations 26–35.

3.4 PostMarket and Lifecycle Security

Cybersecurity responsibilities don't end when a device ships.

Medical devices can remain in service for 7–15 years, and in that time, both the threat landscape and regulatory expectations will evolve.

FDA's guidance makes clear that manufacturers must maintain security throughout the supported lifecycle to protect patients, providers, and healthcare networks.

Ignoring lifecycle security not only risks patient harm, but can also result in regulatory action, product recalls, and loss of hospital trust.

Why Lifecycle Security Matters

- Devices are part of a hospital network.
  A single vulnerable device can be an attack vector for entire clinical environments, disrupting operations or exposing patient data.
- Hospitals and regulators expect active OEM engagement.
  Longterm maintenance and monitoring are no longer optional—they're becoming a buying requirement.
- FDA ties postmarket security to premarket evidence.
  Devices that demonstrate clear monitoring and response processes gain regulatory confidence and faster approvals.

Key Practices for OEMs

1. Event Detection and Logging
    - Devices should log securityrelevant events, such as failed authentication attempts or integrity violations.
    - Event logs support incident response, forensic investigations, and regulatory reporting.
    - Pro Tip: Consider enabling logs to be exported or integrated with hospital SIEM tools for faster detection.
2. Lifecycle Vulnerability Monitoring
    - Establish an ongoing monitoring process to track new vulnerabilities affecting your SBOM components.
    - FDA expects manufacturers to act quickly on emerging risks, requiring timely remediation for critical issues with manufacturers being able to demonstrate risk assessment and response.
    - **Common Pitfall:** Treating vulnerability scanning as a premarketonly activity rather than a continuous lifecycle requirement.
3. Coordinated Vulnerability Disclosure (CVD)
    - Create a formal process to receive, evaluate, and disclose vulnerabilities in coordination with customers and regulators.
    - **Pro Tip:** Publicly listing a CVD policy builds hospital and FDA trust and demonstrates regulatory maturity.
4. Resiliency and Recovery Planning
    - Devices must be able to maintain safe operation under attack or recover quickly to a known good state.
    - Secure reset mechanisms and antitampering recovery procedures support ongoing patient safety.
    - **OEM Insight:** Hospitals increasingly ask for vendor recovery documentation before purchasing connected devices.

OEM Insights and Pitfalls

- Strong lifecycle security reduces longterm costs, avoids emergency patching, and strengthens customer relationships.
- Weak submissions often treat postmarket security as an afterthought, providing no clear monitoring or incident response process.
- **Pro Tip:** Align postmarket monitoring with premarket risk analyses—FDA reviewers appreciate clear lifecycle traceability.

For the complete list of PostMarket and Lifecycle Security recommendations and how DigiCert solutions support each requirement, see Appendix 1 – Recommendations 36–50.

3.5 Using These Recommendations in Submissions

Security is not a checkbox exercise—it is a lifecycle commitment.

By addressing all four security control categories in an integrated way, OEMs can:

- Accelerate FDA approvals by reducing AI requests
- Protect patient safety with proactive cybersecurity measures
- Build longterm hospital trust by demonstrating lifecycle accountability

Manufacturers who treat cybersecurity as core to design, testing, updates, and postmarket operations consistently achieve faster approvals and lower postmarket risk.

4. Practical Guidance for OEMs Preparing FDA Submissions

Achieving FDA cybersecurity compliance is not just about checking boxes—it requires a strategic approach that integrates security into design, testing, updates, and lifecycle management.

Too often, manufacturers treat cybersecurity as a lastminute addon, which leads to costly redesigns, AI (Additional Information) requests, and delayed product launches.

The most successful OEMs follow a lifecycle-oriented strategy that embeds security into every phase of device development and regulatory planning.

4.1 Begin with Secure-by-Design Principles

FDA reviewers favor submissions that demonstrate security from day one.

When a device's architecture shows proactive cybersecurity thinking, it instills confidence that the manufacturer understands both patient safety and regulatory expectations.

Key Insights:

- Start with a security architecture that minimizes attack surfaces—disable unused ports, services, and protocols.
- Integrate hardwarerooted trust early (TPMs, secure elements, or PUFs) to protect keys and verify code integrity.
- Perform threat modeling during design, not after the device is built. FDA reviewers increasingly expect evidence of early risk assessments.

Common Pitfall:

Treating cybersecurity as a late-phase add-on results in AI requests, delayed approvals, and in some cases, full design remediation.

4.2 Make Documentation a Strength, Not an Afterthought

Regulators don't just want to know that a device is secure—they want proof. The strongest submissions tell a security story, mapping risks to mitigations, and mitigations to verifiable test evidence.

Best Practices:

- SBOMs: Maintain complete SBOMs for each release, including all third-party and opensource dependencies
- Traceability: Show how every risk is tied to a mitigation and tested for effectiveness
- Submission Package: Organize test reports, SBOMs, and secure boot verification into a cohesive package

Pro Tip:

A clear, well-structured submission can cut weeks off review cycles by preventing back-and-forth AI requests.

4.3 Plan for Lifecycle Security Before Launch

FDA increasingly evaluates post-market readiness as part of premarket review.

OEMs must show they can respond to vulnerabilities quickly and securely, protecting both patients and clinical networks.

Strategic Steps:

- Implement secure update mechanisms with cryptographic signing, validation, and anti-rollback
- Establish a vulnerability monitoring process tied to your SBOM to respond rapidly to CVEs
- Create a coordinated vulnerability disclosure (CVD) policy to engage hospitals and regulators responsibly

Real World Impact:

Manufacturers with a robust lifecycle plan gain hospital trust and often become the preferred vendor over competitors without clear postmarket strategies.

When a device's architecture shows proactive cybersecurity thinking, it instills confidence that the manufacturer understands both patient safety and regulatory expectations.

4.4 Build an FDA-Ready Submission Process

Successful OEMs don't just secure the device—they secure the review process:

- Map your submission to FDA's four security control categories (Sections 3.1–3.4) for clarity.
- Include executive summaries alongside raw test evidence to help reviewers quickly confirm compliance.
- Maintain a living internal security package so updates and new releases can be submitted without starting from scratch.

Insight:

FDA reviewers are more likely to trust and approve OEMs who demonstrate maturity in both technical security and regulatory communication.

OEM Takeaway:

Treat cybersecurity not as a compliance hurdle, but as a strategic enabler. By doing so, you will:

- Accelerate approvals,
- Reduce post-market risk, and
- Strengthen hospital and regulator confidence in your products.

5. Conclusion: Cybersecurity as a Strategic Advantage

Cybersecurity in medical devices is no longer just a regulatory checkbox—it is a critical component of patient safety, market access, and hospital trust.

The FDA's Cybersecurity Premarket Guidance makes it clear: manufacturers must design, document, and maintain security as an integral part of their product lifecycle.

Manufacturers that succeed do three things well:

1. Integrate security from day one
    - Secure-by-design principles reduce vulnerabilities, avoid costly redesigns, and accelerate FDA approval.
2. Demonstrate security with evidence
    - Complete SBOMs, risk-to-mitigation traceability, and curated test results build reviewer confidence.
3. Commit to lifecycle resilience
    - Ongoing vulnerability monitoring, secure updates, and post-market processes protect patients and networks long after launch.

The Business and Regulatory Payoff

A strong cybersecurity posture is no longer just a safety requirement—it is a competitive differentiator:

- Faster Approvals: Submissions that align with FDA expectations and include clear, verifiable evidence see fewer AI requests and quicker clearances.
- Lower Post-mMarket Risk: A lifecycle security plan reduces the likelihood of recalls, safety notices, and emergency patching.
- Hospital and Market Confidence: Healthcare systems now prefer vendors who can demonstrate long-term cybersecurity stewardship.

Next Steps for OEMs

- Evaluate your current processes against the four security control categories outlined in this whitepaper.
- Identify gaps in your design, documentation, update mechanisms, or post-market monitoring.
- Leverage trusted partners and proven solutions, like DigiCert Device Trust Manager, DigiCert TrustCore SDK, TrustEdge, and DigiCert Software Trust Manager, to accelerate compliance and maintain security throughout the lifecycle.

By embracing cybersecurity as a strategic enabler, OEMs can protect patients, streamline FDA submissions, and strengthen long-term market trust.

For the complete set of FDA recommendations and how DigiCert solutions support compliance, refer to Appendix 1, which provides all 50 recommendations organized by security control category.

Secure FDA Compliance From the Start

Don't wait for regulatory pressure or delayed approvals to expose security gaps. Get ahead of FDA cybersecurity expectations by integrating DigiCert's device trust solutions early in your development cycle. From design through deployment, DigiCert helps you embed identity, integrity, and lifecycle management into every connected device—so you can build secure-by-design products that accelerate approvals and earn long-term trust.

Appendix 1

Item	Appendix 1 Recommendation	Recommendation Text	How DigiCert Helps OEMs to Comply
1	Section A: Authentication	Use cryptographically strong authentication, where the authentication functionality resides on the device, to authenticate personnel, messages, commands updates, and as applicable, all other communication pathways. Hardware-based security solutions should be considered and employed when possible;	✓ Device Trust Manager offers secure credential provisioning policies, ensuring each device has a strong, certificate-backed "birth" identity to avoid spoofing. Device access to certificate issuance, OTA updates, and, policies are strictly controlled through the certificate-backed identity of the device, device group membership, and assignment of policies to the device group. ✓ TrustCore SDK and TrustEdge support hardware TPMs, and hardware-based secure elements ensure keys are always protected. ✓ Device Trust Manager user and API access are strictly controlled, using least-privileges, by a combination of role-based access control, API keys, two-factor authentication, client certificate authentication, and support for popular IDPs.
2	Section A: Authentication	Authenticate external connections at a frequency commensurate with the associated risks. For example, if a device connects to an offsite server, then the device and the server should mutually authenticate each session and limit the duration of the session, even if the connection is initiated over one or more existing trusted channels;	✓ Device Trust Manager offers secure credential provisioning policies, ensuring each device has a strong, certificate-backed "birth" and "operational" certificates which can be used for mutual TLS (mTLS) with DigiCert and non-DigiCert endpoints.
3	Section A: Authentication	Use appropriate user authentication (e.g., multi-factor authentication to permit privileged device access to system administrators, service technicians, or maintenance personnel, among others, as needed);	✓ TrustCore SDK allows OEMs to create cryptographically secure authentication schemes to ensure only authorized users can gain access to the device.
4	Section A: Authentication	Require authentication, and authorization in certain instances, before permitting software or firmware updates, including those updates affecting the operating system, applications, and anti-malware functionality;	✓ Device Trust Manager's granular role-based access control (RBAC) ensures only permitted users and/or service accounts can perform device operations, such as OTA updates. ✓ Software Trust Manager can scan and sign software/ firmware updates that can be verified by the device prior to being installation.
5	Section A: Authentication	Strengthen password protections. Do not use passwords that are hardcoded, default, easily guessed, or easily compromised (e.g., passwords that are the same for each device; unchangeable; can persist as default; difficult to change; and/or vulnerable to public disclosure);	✓ Device Trust Manager offers secure credential provisioning policies ensuring each device has a strong, certificate-backed "birth" identity the eliminates the need for shared or hardcoded credentials.
6	Section A: Authentication	Implement anti-replay measures in critical communications such as potentially harmful commands. This can be accomplished with the use of several methods including the use of cryptographic nonces (an arbitrary number used only once in a cryptographic communication);	✓ TrustCore SDK and TrustEdge support numerous cryptographic methods which can implement anti-replay.

Appendix 1 (continued)

Item	Appendix 1 Recommendation	Recommendation Text	How DigiCert Helps OEMs to Comply
7	Section A: Authentication	Provide mechanisms for verifying the authenticity of information originating from the device, such as telemetry. This is especially important for data that, if spoofed or otherwise modified, could result in patient harm, such as the link between a clinician programmer or monitoring device and an implanted device like a pacemaker, defibrillator, or neurostimulator; or the link between a continuous glucose monitor system and an automated insulin pump;	✓ Device Trust Manager offers secure credential provisioning policies, ensuring each device has a strong, certificate-backed "birth" and "operational" certificates which can be used for mutual TLS (mTLS) between devices and external endpoints. These certificates be managed, including renewal and revocation. ✓ TrustCore SDK can be used to sign telemetry and data transmitted from the device to ensure message data integrity.
8	Section A: Authentication	Do not rely on cyclic redundancy checks (CRCs) as security controls. CRCs do not provide integrity or authentication protections in a security environment. While CRCs are an error detecting code and provide integrity protection against environmental factors (e.g., noise or EMC), they do not provide protections against an intentional or malicious actor; and	✓ TrustCore SDK and TrustEdge support numerous cryptographic methods which can create and verify cryptographic hashes. ✓ Software Trust Manager provides a robust code signing solution, which can include signing of cryptographic hashes.
9	Section A: Authentication	Consider how the device and/or system should respond in event of authentication failure(s).	✕ This requirement falls on the manufacturer to implement. ✓ By default, Device Trust Manager denies all failed device and user logins and logs all these events.
10	Section A: Authentication	Limit authorized access to devices through the authentication of users (e.g., user ID and password, smartcard, biometric, certificates, or other appropriate authentication method);	✕ This requirement falls on the manufacturer to implement. ✓ TrustCore SDK and TrustEdge can support theauthentication of users to a device using certificate-based authentication.
11	Section A: Authentication	Use automatic timed methods to terminate sessions within the medical device system where appropriate for the use environment;	✕ This requirement falls on the manufacturer to implement.
12	Section A: Authentication	Employ an authorization model that incorporates the principle of least privileges by differentiating privileges based on the user role (e.g., caregiver, patient, healthcare provider, system administrator) or device functions; and	✕ This requirement falls on the manufacturer to implement. ✓ Device Trust Manager's granular role-based access control (RBAC) ensures only permitted users and/or service accounts can perform device operations, such as OTA updates.
13	Section B: Authorization	Design devices to "deny by default" (i.e., that which is not expressly permitted by a device is denied by default). For example, the device should generally reject all unauthorized connections (e.g., incoming TCP, USB, Bluetooth, serial connections). Ignoring requests is one form of denying authorization.	✕ This requirement falls on the manufacturer to implement. ✓ By default, TrustEdge ships with no open inbound TCP/UDP service ports, avoiding the need to disable or firewall open ports. Device communication with Device Trust Manager occurs using MQTTs over TLS 1.3 with mTLS authentication.

Appendix 1 (continued)

Item	Appendix 1 Recommendation	Recommendation Text	How DigiCert Helps OEMs to Comply
14	Section C - Cryptography	Select industry-standard cryptographic algorithms and protocols, and select appropriate key generation, distribution, management and protection, as well as robust nonce mechanisms.	✓ Both TrustCore SDK and TrustEdge support all modern symmetric and asymmetric encryption algorithms including NIST- approved PQC algorithms: ML-KEM, ML-DSA and SLH-DSA. TrustCore SDK crypto is also NIST FIP 140-2/3 certified.
15	Section C: Cryptography	Use current NIST recommended standards for cryptography (e.g., FIPS 140-378) or equivalent-strength cryptographic protection that are expected to be considered cryptographically strong throughout the service life of the device. Manufacturers should not implement cryptographic algorithms that have been deprecated or disallowed in applicable standards or best practices (e.g., NIST SP 800-131A, Transitioning the Use of Cryptographic Algorithms and Key Lengths). Implementation of algorithms with a status of "legacy use" should be discussed with FDA during a pre-submission meeting.	✓ Both TrustCore SDK and TrustEdge support all modern symmetric and asymmetric encryption algorithms including the new NIST- approved PQC algorithms: ML-KEM, ML-DSA and SLH-DSA. TrustCore SDK crypto is also NIST FIP 140-2/3 certified.
16	Section C: Cryptography	Design a system architecture and implement security controls to prevent a situation where the full compromise of any single device can result in the ability to reveal keys for other devices. For example, avoid using master-keys stored on device, or key derivation algorithms based solely on device identifiers or other readily discoverable information. For example, avoid using device serial numbers as keys or as part of keys. Device serial numbers may be disclosed by patients seeking additional information on their device or might be disclosed during a device recall to identify affected products and should be avoided as part of the key generation process (e.g., public key cryptography can be employed to help meet this objective).	✓ Both TrustCore SDK and TrustEdge per-device keypairs (RSA, ECC, ML-DSA, etc.) are securely stored in TPM 1.2, TPM 2.0, ARM TrustZone and ephemeral keys created through Physical Unclonable Functions (PUF).
17	Section C: Cryptography	Implement cryptographic protocols that permit negotiated parameters/versions such that the most recent, secure configurations are used, unless otherwise necessary.	✓ Both TrustCore SDK and TrustEdge support negotiated encryption of device data in transit, using TLS 1.3 with ECDH, RSA, ECC, or with ML-KEM, ML-DSA, or SLH-DSA.

Appendix 1 (continued)

Item	Appendix 1 Recommendation	Recommendation Text	How DigiCert Helps OEMs to Comply
18	Section C: Cryptography	Do not allow downgrades, or version rollbacks, unless absolutely necessary for safety reasons, and log and document the event. Downgrades can allow attackers to exploit prior, less protected versions and should be avoided.	✓ Both TrustCore SDK and TrustEdge can be implemented by the OEM to prevent version downgrades.
19	Section D: Code Integrity	Hardware-based security solutions should be considered and employed when possible;	✓ Both TrustCore SDK and TrustEdge support hardware security using TPM 1.2, TPM 2.0, ARM TrustZone and ephemeral keys created through Physical Unclonable Functions (PUF). ✓ Device Trust Manager root and intermediate CA private keys are stored in FIPS-certified HSMs, in data centers subjected to over 30+ audit regimes.
20	Section D: Code Integrity	Authenticate firmware and software. Verify authentication tags (e.g., signatures, message authentication codes (MACs)) of software/firmware content, version numbers, and other metadata. The version numbers intended to be installed should themselves be signed or have MACs. Devices should be electronically and visibly identifiable (e.g., Unique device identifier (UDI), model number, serial number);	✓ Software Trust Manager provides automated software vulnerability scanning and signing for device software/ firmware as part of the OEM's CI/CD process. It can also generate an SBOM as part of the process to show transparency in the software being used by the devices. ✓ Device Trust Manager with TrustEdge enables secure over-the-air updates of signed binaries and content files over MQTTs. These can either be feature updates or security fixes. Updates can be quickly deployed to large groups of devices. Once connected, devices are immediately notified of the update.
21	Section D: Code Integrity	Allow installation of cryptographically authenticated firmware and software updates, and do not allow installation where such cryptographic authentication either is absent or fails. Use cryptographically signed updates to help prevent any unauthorized reductions in the level of protection (downgrade or rollback attacks) by ensuring that the new update represents an authorized version change; One possible approach for authorized downgrades would be to sign new metadata for downgrade requests which, by definition, only happen in exceptional circumstances.	✓ Device Trust Manager with TrustEdge enables secure over-the-air updates of signed binaries and content files over MQTTs. These files can be verified on the device side using TrustCore SDK, or any secure boot loader.
22	Section D: Code Integrity	Ensure that the authenticity of software, firmware, and configuration are validated prior to execution, e.g., "allow-listing" based on digital signatures;	✓ Software Trust Manager can scan and sign binaries, files and firmware to ensure only valid, authentic software is deploy and installed on devices. ✓ Device Trust Manager with TrustEdge enables secure over-the-air updates of signed binaries, firmware and files over MQTTs. These files can be verified on the device side by the operating system, TrustCore SDK, or a secure boot loader.

Appendix 1 (continued)

Item	Appendix 1 Recommendation	Recommendation Text	How DigiCert Helps OEMs to Comply
23	Section D: Code Integrity	Disable or otherwise restrict unauthorized access to all test and debug ports (e.g., JTAG, UART) prior to delivering products; and	✕ This requirement falls on the manufacturer to implement.
24	Section D: Code Integrity	Employ tamper evident seals on device enclosures and their sensitive communication ports to help verify physical integrity.	✕ This requirement falls on the manufacturer to implement.
25	Section D: Data Integrity	Verify the integrity of all incoming data, ensuring that it is not modified in transit or at rest. Cryptographic authentication schemes verify data integrity, but do not verify data validity. Therefore, the integrity of all incoming data should be verified to ensure that it is not modified in transit or at rest;	✕ This requirement falls on the manufacturer to implement. ✓ TrustCore SDK cryptographic capabilities can be used to hash/sign/verify messages.
26	Section D: Data Integrity	Validate that all data originating from external sources is well-formed and compliant with the expected protocol or specification. Additionally, as appropriate, validate data ranges to ensure they fall within safe limits; and	✕ This requirement falls on the manufacturer to implement. ✓ TrustCore SDK cryptographic capabilities can be used to hash/sign/verify messages.
27	Section D: Data Integrity	Protect the integrity of data necessary to ensure the safety and effectiveness of the device, e.g., critical configuration settings such as energy output.	✓ Software Trust Manager can scan and sign binaries, files and firmware to ensure only valid, authentic software is deploy and installed on devices. ✓ Device Trust Manager with TrustEdge enables secure over-the-air updates of signed binaries, firmware and files over MQTTs. These files can be verified on the device side by the operating system, TrustCore SDK, or a secure boot loader.
28	Section D: Execution Integrity	Use industry-accepted best practices to maintain and verify integrity of code while it is being executed on the device. For example, Host-based Intrusion Detection/Prevention Systems (HIDS/HIPS) can be used to accomplish this goal; and	✕ This requirement falls on the manufacturer to implement. ✓ Device Trust Manager with TrustEdge enables secure over-the-air deployment and configuration of HIDS/HIPS software to devices (e.g. OSSEC, Wazuh, etc.) for device monitoring.
29	Section D: Execution Integrity	Carefully design and review all code that handles the parsing of external data using automated (e.g., static and dynamic analyses) and manual (i.e., code review) methods.	✕ This requirement falls on the manufacturer to implement.
30	Section E: Confidentiality	The proper implementation of authorization and authentication schemes as described in Sections A and B of this appendix will generally ensure confidentiality. However, manufacturers should evaluate and assess whether this is the case during their threat modeling and other risk management activities and make any appropriate changes to their medical device systems to ensure appropriate confidentiality controls are in place.	✓ DigiCert Device Trust solutions support robust authorization and authentication schemes. See sections A and B above.

Appendix 1 (continued)

Item	Appendix 1 Recommendation	Recommendation Text	How DigiCert Helps OEMs to Comply
31	Section F: Event Detection and Logging	Implement design features that allow for security compromises and suspected compromise attempts to be detected, recognized, logged, timed, and acted upon during normal use. Acting upon security events should consider the benefit/ risk assessment in accordance with Section 6.5 of AAMI TIR57 or Section 7.4 of ANSI/AAMI SW96 in determining whether it is appropriate to affect standard device functionality during a security event.	✕ This requirement falls on the manufacturer to implement. ✓ Device Trust Manager with TrustEdge enables secure over-the-air deployment and configuration of monitoring software on devices.
32	Section F: Event Detection and Logging	Ensure the design enables forensic evidence capture. 82 The design should include mechanisms to securely create and store log files off the device to track security events. Documentation should include how and where log files are located, stored, recycled, archived, and how they could be consumed by automated analysis software (e.g., IDS). Examples of security events include, but are not limited to, configuration changes, network anomalies, login attempts, and anomalous traffic (e.g., sending requests to unknown entities).	✕ This requirement falls on the manufacturer to implement. ✓ Device Trust Manager with TrustEdge enables secure over-the-air deployment and configuration of monitoring software on devices. ✓ Device Trust Manager supports detailed device management logging of events such as authentication, certificate issuance, renewals, and OTA updates.
33	Section F: Event Detection and Logging	Design devices such that the potential impact of vulnerabilities is limited by specifying a secure configuration. Secure configurations may include endpoint protections, such as anti-malware, firewall/firewall rules, allow-listing, defining security event parameters, logging parameters, physical security detection, and/or HIDS/HIPS.	✕ This requirement falls on the manufacturer to implement. ✓ Device Trust Manager with TrustEdge enables secure over-the-air deployment and configuration of monitoring software, HIDS, scripts, antivirus/anti-malware and system configuration files on devices.

Appendix 1 (continued)

Item	Appendix 1 Recommendation	Recommendation Text	How DigiCert Helps OEMs to Comply
34	Section F: Event Detection and Logging	Design devices such that they may integrate and/or leverage antivirus/anti-malware protection capabilities. These capabilities may vary depending on the type of device and the software and hardware components it contains: For devices that leverage Windows Operating System: Antivirus/anti-malware is recommended on the device. Manufacturers are recommended to qualify multiple options to support user preferences for different options, especially if the device is used in healthcare facility environments. For devices that leverage other Commercial Operating Systems (e.g., Ubuntu, Unix, Linux, Apple, Android): Antivirus/anti-malware may be recommended based on the environment and associated risks of the device. Different operating systems will likely follow a case-by-case determination based on network exposure and risk. For devices that leverage Embedded Operating Systems (e.g., Real-Time Operating Systems, Windows embedded): Antivirus/malware detection/ protection software is generally not needed unless a particular risk or threat is identified that would not be addressed by other expected security controls.	✕ This requirement falls on the manufacturer to implement. ✓ Device Trust Manager with TrustEdge enables secure over-the-air deployment and configuration of monitoring software, HIDS, scripts, antivirus/anti-malware and system configuration files on devices.
35	Section F: Event Detection and Logging	Design devices to enable software configuration management and permit tracking and control of software changes to be electronically obtainable (i.e., machine readable) by authorized users.	✓ Device Trust Manager with TrustEdge enables secure over-the-air deployment and configuration of monitoring software, HIDS, scripts, antivirus/anti-malware and system configuration files on devices. All device update events are logged to Device Trust Manager.
36	Section F: Event Detection and Logging	Design devices to facilitate the performance of variant analyses such that the same vulnerabilities can be identified across device models and product lines.	✓ Software Trust Manager provides automated software validation and vulnerability scanning for device software as part of your CI/CD process. It can also generate an SBOM as part of the process to show transparency in the software being used by the devices. ✓ Software Trust Manager can monitor SBOMs representing the software components installed on a device, and notify development teams once a new CVE is discovered in a dependency, such as an open- source software package.

Appendix 1 (continued)

Item	Appendix 1 Recommendation	Recommendation Text	How DigiCert Helps OEMs to Comply
37	Section F: Event Detection and Logging	Design devices to notify users when malfunctions or anomalous device behavior, including those potentially related to a cybersecurity breach, are detected.	✕ This requirement falls on the manufacturer to implement. ✓ Device Trust Manager with TrustEdge enables secure over-the-air deployment and configuration of monitoring software, HIDS, scripts, antivirus/anti-malware and system configuration files on devices.
38	Section F: Event Detection and Logging	Consider designing devices such that they are able to produce an SBOM in a machine readable format	✓ Software Trust Manager can generate and monitor SBOMs representing the software components installed on a device , and notify development teams once a new CVE is discovered in a dependency, such as an open-source software package.
39	Section G: Resiliency and Recovery	Implement features that protect critical functionality and data, even when the device has been partially compromised. For example, process isolation, virtualization techniques, and hardware-backed trusted execution environments all provide mechanisms to potentially contain the impact of a successful exploitation of a device.	✕ This requirement falls on the manufacturer to implement. ✓ Both TrustCore SDK and TrustEdge support hardware security for private keys using TPM 1.2, TPM 2.0, ARM TrustZone, and ephemeral keys created through Physical Unclonable Functions (PUF).
40	Section G: Resiliency and Recovery	Design devices to provide methods for retention and recovery of trusted default device configuration by an authenticated, authorized user.	✕ This requirement falls on the manufacturer to implement.
41	Section G: Resiliency and Recovery	Design devices to specify the level of resilience, or independent ability to function, that any component of the medical device system possesses when its communication capabilities with the rest of the medical device system are disrupted, including disruption of significant duration.	✕ This requirement falls on the manufacturer to implement.
42	Section G: Resiliency and Recovery	Design devices to be resilient to possible cyber incident scenarios such as network outages, Denial of Service, excessive bandwidth usage by other products, disrupted quality of service (QoS), and/or excessive jitter (i.e., a variation in the delay of received packets).	✕ This requirement falls on the manufacturer to implement.
43	Section G: Resiliency and Recovery	Design devices to be resilient to possible noise items (e.g., scanning).	✕ This requirement falls on the manufacturer to implement.
44	Section F: Firmware and Software Updates	Design devices to anticipate the need for software and firmware patches and updates to address future cybersecurity vulnerabilities. This will likely necessitate the need for additional storage space and processing resources.	✓ The combination of Software Trust Manager, Device Trust Manager and TrustEdge provides an end-to-end solution for firmware/code scanning, signing and over-the-air update to devices, with a minimal device footprint.

Appendix 1 (continued)

Item	Appendix 1 Recommendation	Recommendation Text	How DigiCert Helps OEMs to Comply
45	Section F: Firmware and Software Updates	Consider update process reliability and how update process works in event of communication interruption or failure. This should include both considerations for hardware impacts (timing specifics of interruptions) and which phase of the update process the interruption or failure occurs.	✓ Device Trust Manager and TrustEdge provides a robust system for delivery of over-the-air updates, that is tolerant of network outages, retries, transient network conditions, and large- scale device updates.
46	Section F: Firmware and Software Updates	Consider cybersecurity patches and updates that are independent of regular feature update cycles.	✓ Device Trust Manager and TrustEdge allow for security updates to be delivered to devices independent of feature updates.
47	Section F: Firmware and Software Updates	Implement processes, technologies, security architectures, and exercises to facilitate the rapid verification, validation, and distribution of patches and updates.	✓ Device Trust Manager and TrustEdge allow for scanned, signed updates to be quickly delivered to devices to expedite the rollout of patches and updates.
48	Section F: Firmware and Software Updates	Preserve and maintain full build environments and virtual machines, regression test suites, engineering development kits, emulators, debuggers, and other related tools that were used to develop and test the original product to ensure updates and patches may be applied safely and in a timely manner.	✕ This requirement falls on the manufacturer to implement.
49	Section F: Firmware and Software Updates	Maintain necessary third-party licenses throughout the supported lifespan of the device. Develop contingency plans for the possibility that a third-party company goes out of business or stops supporting a licensed product. Modular designs should be considered such that third-party solutions could be readily replaced.	✕ This requirement falls on the manufacturer to implement. ✓ Both TrustCore SDK and TrustEdge are open source, which allows OEMs access to the source code access. ✓ All DigiCert Device Trust solutions are built upon proven industry standards such as HTTP/REST, TLS 1.3, EST, SCEP, CMPv2, ACME, MQTT, RSA, ECC, ML-KEM, ML-DSA, SLH-DSA, and many others.
50	Section F: Firmware and Software Updates	Implement a secure process and mechanism for providing validated software updates and patches for users.	✓ Device Trust Manager with TrustEdge enables secure over-the-air updates of binaries and configuration file updates over MQTTs. Updates can be packaged to include the ability to notify users, support opt-out, and postpone updates.

Get Started with DigiCert Today

The path to FDA cybersecurity compliance doesn't need to be complex. DigiCert helps you build a scalable, trusted device ecosystem with premarket and postmarket readiness in mind. Our solutions are already supporting leading medical device manufacturers in achieving FDA alignment—without delaying innovation or time to market. Contact us today to speak with a compliance expert or request a personalized Device Trust assessment.

Ready to get started?

Scan the QR Code

Email: device-trust@digicert.com
Visit: digicert.com/device-trust