



GUIDE

The MedTech Cybersecurity Standards Decoder

A plain-English field guide to FDA Section 524B, IEC 81001-5-1, AAMI TIR57, ANSI/AAMI SW96, ISO 14971, and 8 more medical device cybersecurity standards. What they require, how they connect, and what

Twelve standards. One section each. Same template every time: What it is · What it requires · What the FDA expects to see · How it connects.

How to read this section. If a standard is in your scope, the “What the FDA expects to see” line tells you the artifact you must produce. The “How it connects” line tells you which other standards feed into or out of it. Use Part 3 to see the whole web at once.

Standard 1 of 12 - FDA · 21 USC §524B + Feb 3, 2026 Premarket Guidance

FDA Premarket Cybersecurity Requirements

Applies to: Every “cyber device” submission (510(k), De Novo, PMA, IDE, BLA).

What it is

The federal statute and its implementing guidance. Section 524B (added by the Consolidated Appropriations Act, 2023) requires cybersecurity documentation in every premarket submission for a “cyber device.” The February 3, 2026 final guidance replaced the 2023 draft and defines the seven-section submission format the FDA now enforces at Technical Screening.

What it requires

- A Secure Product Development Framework (SPDF) covering the full lifecycle.
- A plan to monitor, identify, and address postmarket vulnerabilities.
- Evidence the device and related systems are reasonably secure.
- A Software Bill of Materials (SBOM) including all commercial, open-source, and off-the-shelf components.

What the FDA expects to see

A complete cybersecurity submission package mapped to the seven sections of the February 3, 2026 guidance. Reviewers check completeness at Technical Screening before the 180-day clock starts. Missing sections = automatic RTA.



How it connects

Section 524B is the umbrella. Every other standard in this guide is one of the bricks. AAMI TIR57 / SW96 handles risk. IEC 81001-5-1 handles the SPDF. IEC 62304 handles the software lifecycle. They all land in one eSTAR cybersecurity section.

Standard 2 of 12 - FDA eSTAR v6 · Cybersecurity Section

eSTAR Cybersecurity Submission

Applies to: 510(k) and De Novo submissions filed via eSTAR (mandatory).

What it is

eSTAR is the FDA's interactive PDF that has replaced the legacy 510(k) format (mandatory for 510(k)s since October 2023; mandatory for De Novos since October 1, 2025). The current major version is nIVD/IVD eSTAR Version 6 (with minor releases such as v6.1 for QMSR alignment effective February 2, 2026, and v6.2). The cybersecurity section is structured - specific upload slots for specific documents, in a specific order.

What it requires

- Security architecture description with labeled network interfaces, data flows, and trust boundaries.
- Threat model using a structured framework (STRIDE or equivalent) with explicit threat-to-mitigation mapping.
- SBOM in SPDX or CycloneDX format, conformant to NTIA Minimum Elements, with vulnerability status per component.
- Cybersecurity risk assessment + Secure Product Development Framework (SPDF) documentation.
- Full-scope penetration test report with remediation disposition for every finding at every severity level.
- Vulnerability management plan with formal CVD policy and a documented secure update mechanism.
- Postmarket monitoring & patching plan, plus cybersecurity labeling for the user.

What the FDA expects to see

Every cybersecurity field populated and consistent with attached documentation. Missing uploads or checkbox/document mismatches = early Technical Screening hold (180 days). PDFs must be PDF 1.4 / 1.7 / PDF/A-1a, with embedded fonts, alphanumeric file names, and internal bookmarks for cross-references.

How it connects

eSTAR is the delivery mechanism for everything else in this guide. Each upload slot is fed by one or more underlying standards. Note: section letters have shifted between eSTAR major versions - always verify against the version you've downloaded from FDA.



| **Standard 3 of 12 - AAMI TIR57:2016 (R2023)**

Principles for Medical Device Security - Risk Management

Applies to: Cybersecurity risk management for any medical device.

What it is

The MedTech-specific extension of ISO 14971 for cybersecurity. TIR57 is how you do security risk management - asset identification, threat analysis, vulnerability assessment, risk evaluation, and risk control - in a way the FDA recognizes and expects.

What it requires

- Identification of cybersecurity assets, threats, and vulnerabilities.
- Estimation of likelihood and severity using a security-aware scheme.
- Risk evaluation and decisions on acceptability.
- Risk control measures with verification.
- A documented, traceable risk file separate from but linked to the ISO 14971 safety file.

What the FDA expects to see

A Cybersecurity Risk Assessment that follows TIR57 (or ANSI/AAMI SW96) structure. The assessment must cover every interface and every component in the SBOM. It must trace threats to mitigations and include a residual risk acceptability statement.

How it connects

TIR57 is the operational manual for the security side of risk management. It feeds the threat model, the risk assessment, and the security architecture - all required eSTAR uploads. ANSI/AAMI SW96 (Standard 5) is the updated alternative.

| **Standard 4 of 12 - AAMI TIR97:2019**

Principles for Medical Device Security - Postmarket Risk Management

Applies to: Any cleared/approved device with a cybersecurity profile.

What it is

The postmarket companion to TIR57. Tells you how to keep doing security risk management after the device ships - CVE monitoring, vulnerability triage, patch management, coordinated disclosure, and MDR/ MedWatch integration.



What it requires

- A postmarket cybersecurity surveillance program (CVE monitoring, threat intel, customer reports).
- A vulnerability triage process tied to your TIR57 / SW96 risk file.
- Coordinated vulnerability disclosure (CVD) consistent with ISO/IEC 30111 and 29147.
- Defined criteria for when a vulnerability requires patching, mitigation, or recall.
- MedWatch reporting integration when patient harm is foreseeable.

What the FDA expects to see

A Cybersecurity Management Plan that operationalizes TIR97 - it must show who monitors what, on what cadence, and how new vulnerabilities are triaged, patched, and disclosed. Patch cadence expectations: critical CVEs within 30 days, high within 60, medium/low in planned releases.

How it connects

TIR97 closes the loop on TIR57. It feeds the vulnerability management plan in the eSTAR cybersecurity section and is the backbone of any postmarket surveillance argument to the FDA.

| Standard 5 of 12 - ANSI/AAMI SW96:2023

Standard for Medical Device Security - Security Risk Management

Applies to: Full lifecycle security risk management for medical devices.

What it is

The newer (2023) consensus standard that consolidates and updates TIR57 and TIR97 into a single, harmonized security risk management framework. The FDA's February 3, 2026 guidance explicitly references SW96 alongside TIR57 as acceptable frameworks.

What it requires

- A documented security risk management process spanning premarket and postmarket.
- Asset, threat, vulnerability, and risk identification methodology.
- Risk acceptance criteria reviewed by management.
- Verification that risk controls work as intended.
- Traceability between security risks and safety risks (ISO 14971 alignment).

What the FDA expects to see

Either a TIR57+TIR97 stack or a SW96-conformant program. SW96 is the cleaner answer for new devices because it's a single standard with a single traceability spine. Reviewers want to see explicit standard citation in the risk file header.



How it connects

SW96 is the convergence standard. It replaces the need to cite TIR57 and TIR97 separately. Still requires ISO 14971 alignment for the safety-security interface and feeds the same eSTAR uploads as TIR57+TIR97.

| Standard 6 of 12 - ISO 14971:2019 + ISO/TR 24971

Risk Management for Medical Devices

Applies to: Every medical device. The bridge between safety and security.

What it is

The foundational risk management standard for medical devices - the one your QMS already lives in. Cybersecurity harms (data breach, device malfunction via cyber attack, patient injury from compromised therapy) are hazardous situations under ISO 14971. Cybersecurity controls that could create new safety hazards must also be evaluated here.

What it requires

- Risk management process integrated into the device lifecycle.
- Hazard identification, risk estimation, and risk evaluation.
- Risk control measures verified for effectiveness.
- Overall residual risk acceptability decision.
- Risk management report signed by management.

What the FDA expects to see

An ISO 14971 risk file that explicitly includes hazardous situations originating from cybersecurity vulnerabilities. The file must be cross-referenced to the TIR57/SW96 security risk file. Reviewers will look for the connection - if it's not there, expect a deficiency.

How it connects

ISO 14971 is the spine. TIR57/SW96 produces the security side of the inputs. IEC 62304 produces the software anomaly side. All three feed a single unified risk file that covers both safety and security in the eSTAR submission.

| Standard 7 of 12 - IEC 62304:2006/AMD1:2015

Medical Device Software - Software Lifecycle Processes

Applies to: Any device containing software (Class A, B, or C).



What it is

The software lifecycle standard for medical devices. Defines what “controlled software development” means - planning, requirements, architecture, detailed design, implementation, integration, system testing, maintenance, and problem resolution. IEC 62304 is required for any device with software, and its SOUP (Software of Unknown Provenance) list is the direct input to the SBOM.

What it requires

- Software development planning with safety classification (A/B/C).
- Requirements management and software architecture documentation.
- Coding, integration, and system-level testing per the safety class.
- SOUP (Software Of Unknown Provenance) identification and risk control.
- Problem resolution, change control, and configuration management records.

What the FDA expects to see

A complete IEC 62304 software lifecycle file - including SOUP list, anomaly reports, and configuration management records. The SOUP list must be reconciled against the SBOM. Mismatches between the SOUP list and SBOM are a common deficiency.

How it connects

IEC 62304 governs how software is built. IEC 81001-5-1 (Standard 8) overlays security activities on top of the IEC 62304 lifecycle. The SOUP list feeds the SBOM. Anomaly reports feed the risk file. Everything lands in the eSTAR software documentation and cybersecurity sections.

| Standard 8 of 12 - IEC 81001-5-1:2021

Health Software & Health IT Systems Safety, Effectiveness and Security - Security

Applies to: Any health software, including medical device software.

What it is

The Secure Product Development Framework (SPDF) standard. FDA's February 3, 2026 guidance explicitly references IEC 81001-5-1 as the SPDF framework. It maps security activities - threat modeling, security requirements, secure design, security verification, vulnerability management - to each phase of the IEC 62304 lifecycle.

What it requires

- Security activities mapped to each phase of the IEC 62304 lifecycle.
- Threat modeling and security risk management throughout development.
- Secure design, secure coding practices, and security verification.



- Software composition analysis (feeds SBOM).
- Security update and patch management process.
- Decommissioning and end-of-life security activities.

What the FDA expects to see

An SPDF document that maps every IEC 81001-5-1 activity to where in your QMS it lives. Reviewers will check that the SPDF is not a template - it must be device-specific and trace to your actual procedures and records.

How it connects

IEC 81001-5-1 is the SPDF answer for FDA. It overlays IEC 62304 (Standard 7) with security. It produces inputs for the threat model, the SBOM, and the vulnerability management plan. IEC 62443-4-1 (Standard 9) is the industrial-controls alternative.

| Standard 9 of 12 - IEC 62443-4-1:2018

Security for Industrial Automation and Control Systems - Product Development Requirements

Applies to: Secure development lifecycle for connected products (often cited alongside 81001-5-1).

What it is

The industrial-controls-world cousin of IEC 81001-5-1. Many MedTech companies, especially those with IoT or OT components, use IEC 62443-4-1 as their SPDF framework. The FDA accepts it as SPDF evidence when the mapping to medical device cybersecurity requirements is explicit.

What it requires

- A documented Secure Development Lifecycle (SDL) with eight practices.
- Threat modeling and security requirements management.
- Secure-by-design architecture and secure coding standards.
- Security verification and validation testing.
- Defect management and security update management.
- Process verification - independent assessment that the SDL is followed.

What the FDA expects to see

The FDA accepts IEC 62443-4-1 conformance as evidence of an SPDF, particularly when paired with an explicit mapping to the February 3, 2026 guidance sections. Third-party SDL assessments (not full certification) are acceptable and add credibility.



How it connects

IEC 62443-4-1 is an alternative or complement to IEC 81001-5-1. Pick one as your SPDF answer. Some companies use 62443-4-1 for OT/IoT components and 81001-5-1 for the software layers. Both feed the same eSTAR SPDF upload slot.

Standard 10 of 12 - UL 2900-1 / UL 2900-2-1

Software Cybersecurity for Network-Connectable Products

Applies to: Network-connectable medical devices (UL 2900-2-1 is the MedTech profile).

What it is

A testable cybersecurity standard with a defined laboratory evaluation methodology. UL 2900-2-1 is the medical device profile. A UL 2900-2-1 evaluation produces a test report that can serve as the cybersecurity testing artifact in the eSTAR submission.

What it requires

- Software weakness analysis (CWE-based static and dynamic testing).
- Vulnerability analysis (CVE matching against the SBOM).
- Penetration testing against the device's exposed interfaces.
- Risk control assessment and security risk management evidence.
- Documented security capabilities (auth, crypto, audit, etc.).

What the FDA expects to see

A UL 2900-2-1 evaluation report can serve as the cybersecurity testing artifact in the eSTAR cybersecurity section. The FDA has recognized UL 2900-2-1 in multiple guidance documents. The report must be current and cover the as-submitted device configuration.

How it connects

UL 2900 is a testing & evidence standard, not a process standard. It validates what your SPDF (IEC 81001-5-1 or 62443-4-1) produced. It consumes the SBOM and the threat model as inputs and produces the pen test report as output.

Standard 11 of 12 - NIST SP 800-115 + 800-30 + CVSS v3.1/v4.0

Security Testing & Vulnerability Scoring Methodology

Applies to: How penetration testing and vulnerability scoring should be performed.



What it is

The reference methodology the FDA expects pen testers to follow (800-115) and the scoring system (CVSS) for prioritizing vulnerabilities. NIST 800-30 provides the risk assessment methodology referenced in the February 3, 2026 guidance.

What it requires

- Pen test reports that follow NIST 800-115 phases (planning, discovery, attack, reporting).
- Threat-informed test scope tied to your threat model (TIR57/SW96 outputs).
- Vulnerabilities scored with CVSS and contextualized for MedTech (medical impact, not just IT impact).
- Risk assessment rationale per NIST 800-30 where applicable.
- Independent tester credentials documented in the report.

What the FDA expects to see

A pen test report that names the methodology, lists the test scope, ties findings to threat model entries, scores every finding with CVSS (with medical context), and documents the remediation disposition - fixed, mitigated, or accepted with rationale - for every finding at every severity level.

How it connects

NIST 800-115 / CVSS feed the testing portion of the eSTAR cybersecurity section. They consume outputs from the threat model (TIR57/SW96) and SBOM (CVE matching) and produce the pen test report that goes into the eSTAR testing upload slot.

Standard 12 of 12 - EU MDR 2017/745 + IVDR 2017/746 + MDCG 2019-16

EU Cybersecurity Expectations for Medical Devices

Applies to: Any device CE-marked or planning to enter the EU/UK markets.

What it is

The EU's regulatory framework for medical devices, with cybersecurity expectations laid out primarily in MDR Annex I (General Safety and Performance Requirements, GSPR 17) and the MDCG 2019-16 guidance document.

What it requires

- IT security in the design and manufacture of the device (MDR Annex I, GSPR 17.2).
- Minimum requirements for hardware, IT network characteristics, and IT security measures (GSPR 17.4).
- Documentation in the technical file demonstrating cybersecurity assessment.
- Postmarket surveillance integrating cybersecurity (PSUR / PMSR).



- Coordinated vulnerability disclosure expectations consistent with ENISA guidance.

What the FDA expects to see

The FDA does not require MDR - but a Notified Body certificate aligned with MDCG 2019-16 is strong secondary evidence of cybersecurity rigor, especially in PMAs or for Breakthrough Device submissions where FDA reviewers apply heightened scrutiny.

How it connects

EU MDR/IVDR is a parallel regulatory regime. The good news: the underlying standards (ISO 14971, IEC 81001-5-1) are shared. A well-built FDA cybersecurity package gets you 80%+ of the way to MDCG 2019-16 conformance. Build once, file in both markets.

Ready to talk through your roadmap?

[Book a Strategy Session →](#)

Source guide: the-medtech-cybersecurity-standards-decoder. For the most current version, visit bluegoatcyber.com/guides/the-medtech-cybersecurity-standards-decoder.