GUIDE

Premarket FDA Cybersecurity Submission Checklist (2026)

Item-by-item checklist for the cybersecurity content of an FDA premarket submission. Eight artifacts, sub-items per artifact, traceability requirements, AI/ML add-ons, and the read-through criteria a reviewer applies.

TL;DR

- Use this as the final pre-upload check against the February 2026 final premarket cybersecurity guidance.
- Every item below is a specific reviewer expectation - not a nice-to-have.
- AI/ML devices need the additional items in the AI section.
- If you cannot tick every box, you have a likely deficiency.

1. Security risk assessment

- [ ] Aligned to AAMI TIR57 / ANSI/AAMI SW96.
- [ ] Integrated with the ISO 14971 risk file (not parallel).
- [ ] Identifies asset, threat, vulnerability, control, residual risk per row.
- [ ] Maps each row to a patient-harm category.
- [ ] Signed and dated by the security risk lead.

2. Threat model

- [ ] Scope statement, asset inventory present.
- [ ] Four architecture views: global, multi-patient harm, updateability, security use-case.
- [ ] Trust boundaries consistent across views.
- [ ] STRIDE per element (or comparable methodology).
- [ ] Control catalog with implementation reference and verification evidence per control.
- [ ] Traceability matrix: threat → control → verification → residual risk → ISO 14971 harm.

3. SBOM

- [ ] Machine-readable: CycloneDX 1.4+ or SPDX 2.3+.
- [ ] NTIA minimum elements present per component.
- [ ] Transitive dependencies enumerated.
- [ ] Cloud backend components included.
- [ ] Mobile companion app components included.
- [ ] Vulnerability disclosure path per component.
- [ ] VEX or equivalent triage statement attached.
- [ ] Hash and EOS date per component.

4. Penetration test report

- [ ] Full attack surface coverage: firmware, hardware, wireless, mobile, APIs, cloud.
- [ ] White-box methodology documented.
- [ ] Letter of Attestation signed by engagement lead.
- [ ] Per-finding: severity (CVSS + clinical impact), reproduction, evidence, remediation, status.
- [ ] High/critical findings retested after remediation.
- [ ] Traceability appendix linking findings back to threat-model entries.
- [ ] Standards cited: NIST SP 800-115, OWASP MASVS/ASVS, FDA 2026 guidance, AAMI TIR57.

5. Architecture views (delivered as standalone artifact)

- [ ] Global system view diagram + narrative.
- [ ] Multi-patient harm view diagram + narrative.
- [ ] Updateability view diagram + narrative (key management, signing, rollback).
- [ ] Security use-case view (states, transitions, threat behavior).
- [ ] Each view annotated with trust boundaries and data classification.

6. Cybersecurity labeling

- [ ] Patient-facing security information present (where applicable).
- [ ] Clinician/operator-facing security information present.
- [ ] Network and connectivity assumptions documented.

- [ ] User-actionable security configuration steps documented.
- [ ] CVD program contact information.

7. Postmarket cybersecurity management plan

- [ ] Vulnerability monitoring sources defined.
- [ ] Triage SLA documented (target: 5 business days post-discovery).
- [ ] Patch deployment cadence by severity defined.
- [ ] CVD program documented with intake, triage, and disclosure SLAs.
- [ ] SBOM regeneration cadence (every build).
- [ ] End-of-support tracking process.
- [ ] Customer communication process for vulnerabilities and patches.
- [ ] Named owners for each function.

8. Predicate-comparison cybersecurity narrative (510(k) only)

- [ ] Predicate cyber surface enumerated.
- [ ] New-device cyber surface enumerated.
- [ ] Delta identified (every interface added beyond predicate).
- [ ] New threats arising from delta.
- [ ] Controls mitigating new threats.

AI/ML add-on items (when applicable)

- [ ] AI-DSF section per January 2025 draft guidance.
- [ ] Model card / transparency content in labeling.
- [ ] Subgroup performance breakdowns.
- [ ] AAMI CR34971 alignment in risk file.
- [ ] AI-specific cybersecurity threats addressed (data poisoning, evasion, inversion, prompt injection) with MITRE ATLAS / OWASP ML Top 10 mapping.
- [ ] Foundation models and third-party AI APIs in SBOM and supplier evaluation.
- [ ] PCCP if model will change postmarket.
- [ ] Performance and bias monitoring plan tied to PCCP.

Final reviewer-eye read-through

- [ ] A senior MedTech regulatory reader (not the author) can answer in 15 minutes from the package alone: what does the device do, what are the cyber threats, how are they controlled.
- [ ] Cross-references between artifacts resolve.
- [ ] Versions and dates consistent across artifacts.
- [ ] No "TBD" or placeholder content.

Frequently asked questions

Is this checklist applicable to De Novo and PMA too?

Yes for items 1-7 and the AI add-ons. Item 8 (predicate comparison) is 510(k)-specific - De Novo replaces it with a security-architecture-justification, PMA folds it into the deeper modular content.

Can I file with TBDs and complete in the AI letter?

Technically yes; practically a recipe for a longer review cycle. Each TBD is a deficiency the reviewer will flag - and the AI letter clock starts running before you have the answer ready.

How is this different from the 2023 draft checklist?

Tighter expectations on architecture views, explicit Letter of Attestation expectation, clearer postmarket cadence requirements, and AI alignment.

What is the most-skipped item in real submissions?

Multi-patient harm view. Teams build the global view and the security use-case view but skip multi-patient harm because they think "one device per patient" - reviewers ask anyway because cloud and OTA aggregate risk.

Do I need a separate cybersecurity labeling document or is it inside the IFU?

Either works. What matters is that the security information is identifiable and complete. Many manufacturers use a separate "Cybersecurity Information for Operators" document referenced from the IFU.

Where does the CVD program go in the package?

Postmarket cybersecurity management plan section. Public-facing CVD policy URL referenced from the labeling.

What proves my postmarket plan is operational, not just written?

Sample vulnerability triage records, SBOM regeneration evidence, patch release history (where available pre-clearance from beta or earlier products), CVD intake examples. Reviewers do not require all of this at premarket but they do appreciate evidence the plan is more than paper.

How do we handle items where the answer depends on the hospital configuration?

Document the assumption explicitly in the cybersecurity labeling and the threat model. Assumptions are acceptable when they are visible; hidden assumptions cause deficiencies.

Do we need to include the SBOM source files (e.g., go.mod, package.json)?

No, the generated CycloneDX/SPDX file is sufficient. Source manifests may be requested if the SBOM looks incomplete.

Can we re-use evidence from a previous submission?

Yes for shared platforms or families - with explicit reference and a delta analysis showing what changed. Stale evidence reused without delta analysis is a frequent deficiency.

Where to go next

- How to Pass FDA 510(k) Cybersecurity on the First Submission
- FDA Cybersecurity Deficiency Letter Response Playbook
- FDA Premarket Cybersecurity Service

Ready to talk through your roadmap?

Book a Strategy Session →

Source guide: premarket-fda-cybersecurity-submission-checklist. For the most current version, visit bluegoatcyber.com/guides/premarket-fda-cybersecurity-submission-checklist.