BLUE GOAT CYBER
Medical Device Cybersecurity · FDA Specialists

LEGACY MEDICAL DEVICE CYBERSECURITY PLAYBOOK

The Legacy Medical Device Cybersecurity Playbook

Bring fielded legacy devices up to current FDA expectations: risk assessment, compensating controls, EOL communications, remediation tiers.

bluegoatcyber.com · 100% FDA submission success rate

LEGACY & REMEDIATION

The legacy medical device cybersecurity playbook.

Most fielded medical devices were not designed to meet the FDA's 2026 cybersecurity expectations. Pulling them all from the field is unrealistic; ignoring them is a regulatory and patient-safety risk. The middle path - structured remediation with compensating controls and honest customer communications - is what the FDA, hospitals, and patients expect.

Key takeaway: 'Legacy' is not a defense. The FDA expects manufacturers to actively manage cybersecurity risk for fielded devices throughout the total product lifecycle, regardless of when they were cleared.

1. Inventory and risk-rank your fielded fleet

- Catalog every cleared SKU still in clinical use, with software/firmware versions.
- Map known CVEs against an SBOM (build one retroactively if needed).
- Score each model: connectivity, patient-safety impact, install base, patchability.
- Group into tiers: **Tier 1** (active patch), **Tier 2** (mitigate), **Tier 3** (EOL plan).

2. Risk-assessment template (10 columns)

- Device family / SKU
- Software/firmware version in field
- Connectivity profile (BLE, Wi-Fi, cellular, USB, none)
- Install base estimate
- Highest CVSS for unpatched component
- Clinical impact category (life-supporting, therapeutic, monitoring, diagnostic)
- Patchability (full, partial, configuration-only, none)
- Compensating controls available
- Tier assignment
- Owner + next review date

3. Compensating controls when you can't patch

Network segmentation	Provide hospital biomed teams with a VLAN guidance doc and required ACLs.

Disable unused services	Field configuration patch removes dormant ports/services. Lowest-risk change.
Strengthen authentication	Enforce non-default credentials; force change at first deploy. Document.
Add monitoring	Provide IDS signatures + syslog forwarding config. Hospitals run the SIEM.
Physical controls	Lock cabinets, port blockers, tamper-evident seals - low-tech but effective.

4. Customer communications that build trust

- Proactive advisory whenever a CVE materially affects fielded devices.
- Plain-language clinical impact statement - not just CVSS.
- Concrete mitigation steps the hospital biomed team can apply *today*.
- Patch ETA, or honest 'no patch planned - here's why and what to do'.
- Updated MDS^2 form with current security posture.
- Single advisories page on your website with timeline of updates.

5. The EOL / EOS decision framework

Trigger criteria	Age in market, exploit landscape, replacement availability, ongoing support cost.
Notice period	Minimum 12 months written customer notice with documented support sunset.
Migration path	Provide path to current-generation device. Trade-in / loaner programs build goodwill.
Residual risk	Document risk acceptance for customers who continue use beyond EOS.
Regulatory comms	Notify FDA where appropriate (recall vs. EOS classification matters).

6. Tiered remediation roadmap (example)

- **Tier 1 (active patch):** 90-day patch cycle, customer advisory at release.
- **Tier 2 (mitigate):** compensating controls within 60 days; monitor for new threats.
- **Tier 3 (EOL plan):** 12-month sunset, migration program, final security advisory at EOS.
- Reassess tier assignment quarterly - threats and exploit landscape change.

7. What FDA expects in postmarket reports on legacy devices

- Evidence that you actively monitor your fielded fleet (not just newest SKUs).
- Documented compensating controls when patches aren't available.
- Customer communications that show transparency, not minimization.
- Risk-based prioritization tied to ISO 14971.
- Clear EOL plans for devices no longer supportable.

Key takeaway: The fastest way to lose hospital trust - and FDA goodwill - is silence on a known issue. Even a 'no fix planned, here's why' advisory beats no advisory at all.

READY FOR THE NEXT STEP?

Talk to a senior medical device security engineer.

We've contributed cybersecurity documentation, threat models, SBOMs, and pen test reports to **250+ FDA submissions** across 510(k), De Novo, and PMA pathways - with a **100% submission success rate**. If you're building a cyber device and want to go in with airtight artifacts on the first try, we should talk.

Book a legacy device working session
30 minutes. No slide deck. Bring your device profile and your top three questions.

bluegoatcyber.com/contact

WHAT WE DO

- **FDA premarket cybersecurity** - SPDF, threat model, SBOM, pen test, security risk assessment, eSTAR-ready package
- **FDA cybersecurity deficiency response** - rapid remediation when reviewers send a letter
- **Postmarket programs** - vulnerability monitoring, VEX, coordinated disclosure, patch validation
- **Legacy device remediation** - bring older devices up to current FDA expectations