BLUE GOAT CYBER
Medical Device Cybersecurity

CHECKLIST

FDA Premarket Cybersecurity Package Readiness Checklist

Book a free discovery call
30 minutes with a senior expert
bluegoatcyber.com/discovery-call

Readiness checklist | Reviewed October 17, 2026

A planning aid for your device-specific scope, not a universal list of mandatory documents or a guarantee of clearance. Mark items complete, open, or not applicable with a documented rationale.

1. Define the scope

Record intended use, submission pathway, target date, and product configuration.

Inventory firmware, apps, cloud services, interfaces, accessories, and third-party components.

Assess the Section 524B cyber-device criteria and covered pathway. IDE applications are not Section 524B marketing submissions.

2. Build a traceable evidence set

Document secure development activities, security requirements, and architecture.

Prepare the threat model and cybersecurity risk assessment, including patient-harm consequences.

Prepare architecture views appropriate to the device and risk, including multi-patient and update risks where applicable.

Prepare the SBOM, component support information, and product-specific vulnerability assessment. Do not infer VEX status without evidence.

3. Test and review

Agree the security test scope, access, configurations, and environment.

Trace security testing and penetration testing evidence to threats and controls.

Document findings, mitigations, unresolved anomalies, and the risk-owner review. Retests cover findings with uncontrolled risk.

4. Prepare the submission and handoff

Prepare cybersecurity labeling and a vulnerability management plan covering monitoring, coordinated disclosure, and updates.

Map applicable evidence into the current submission format. eSTAR v7.1 applies where the pathway uses eSTAR; IDE work goes in the investigational plan.

Agree responsibility for cybersecurity deficiency responses and postmarket activities.

Treat MDS2 as optional procurement disclosure, not an FDA or eSTAR requirement.

Sources and next step

FDA final premarket cybersecurity guidance, February 3, 2026: fda.gov/media/119933/download. Binding requirements: FD&C Act Section 524B. Guidance recommendations and applicability must be assessed for the specific device.

Discuss your scope: bluegoatcyber.com/services/fda-premarket-cybersecurity-services

Talk to a senior medical device cybersecurity expert

Book a free 30-minute discovery call. Scan the code or visit bluegoatcyber.com/discovery-call. You get a written quote within 24 hours.

Informational material. Confirm requirements for your device and market. The manufacturer owns risk decisions, QMS approvals, and regulatory submissions. No regulatory outcome is promised.