



# Early-Stage Cybersecurity Readiness Checklist

*For connected wearable, mobile application, and cloud platforms: prototype through pre-submission.*

*This checklist covers the cybersecurity items worth thinking through now, while your hardware and software design are still moving, so decisions stay cheap to change. It is a starting point, not a substitute for a full threat model, risk assessment, or FDA premarket cybersecurity documentation package.*

*The FDA recommends building cybersecurity into a device through a Secure Product Development Framework (SPDF): a lifecycle approach that starts at initial design and continues through disposal, covering the device's full Total Product Life Cycle (TPLC). The items below are organized around the early, prototype-stage questions that feed into that framework, so the formal SPDF activities (threat modeling, security risk assessment, SBOM, and the rest of the full premarket package) have a running start when you are ready for them.*

## 1. Intended Use and Device Classification

- ☐ Document the intended use for each function of the device (for example, a diagnostic or monitoring function alongside a general wellness feature), separately.
- ☐ If the device combines a medical device function with a non-medical function, write down the rationale for how the two are isolated from each other.
- ☐ Note any wireless or radio frequency interface, including Bluetooth, even where a given function does not use it.
- ☐ Confirm your intended FDA submission pathway with your regulatory team once it is settled; cybersecurity documentation expectations follow from that pathway.

Why this matters. Section 524B of the Federal Food, Drug, and Cosmetic Act tests what the device is capable of, not only how a specific feature is intended to be used, and explicitly lists radio frequency and inductive interfaces. A wellness feature that shares hardware and connectivity with a medical function does not fall outside that scope simply because it can be turned off. FDA's guidance on Multiple Function Device Products speaks directly to isolating a regulated function from an unregulated one; that is the right reference point for your rationale.

## 2. Hazard Analysis and the Cybersecurity Connection

- ☐ Start, even informally, a short list of your device's hazards: ways it could harm a patient, independent of whether a cyberattack is involved (for example, a wrong sensor reading leading to a wrong treatment decision).
- ☐ Keep that list separate from your cybersecurity threat list for now. A hazard analysis is a patient-safety deliverable owned by your team under ISO 14971, not something Blue Goat produces for you.
- ☐ As you build your threat list in Section 5 below, flag anywhere a cyber threat could cause one of these hazards to occur. That link, threat leads to control leads to test leads to patient harm, is the traceability spine your formal threat model and risk assessment will document in detail.

Why this matters. Blue Goat will ask for your hazard analysis alongside your intended use and system architecture as one of the three starting inputs for any cybersecurity guidance. The FDA keeps patient-safety severity (ISO 14971, owned by your team) and cybersecurity exploitability (scored separately, see Section 5) on two distinct axes. Starting both lists now, even roughly, means the formal versions have a running start instead of being built from scratch.

### 3. System Architecture and Data Flow Diagram (DFD)

- ☐ Sketch, even at a high level, how data moves: wearable to mobile application to cloud.
- ☐ Record the connectivity used at each hop (for example, Bluetooth from wearable to phone; Wi-Fi or cellular from phone to cloud).
- ☐ Turn that sketch into a lightweight data flow diagram using DFD3 (Shostack's five-element model): external entities (user, cloud provider), processes (the app, the firmware), data stores (local cache, cloud database), dataflows connecting them, and a trust boundary wherever data crosses from one party's control to another, such as device to phone or phone to cloud.
- ☐ Once you select a cloud provider, document its security posture and where its responsibility ends and yours begins.
- ☐ Note any third-party components, libraries, or software you do not control, even at the prototype stage. For each one, start tracking its support status (actively maintained, no longer maintained, or abandoned) and its end-of-support date. The FDA requires both, beyond the component list itself, in a future Software Bill of Materials (SBOM), and they are far easier to capture as you adopt each component than to reconstruct later.

Why this matters. A DFD is the structure your formal threat model will be built on; STRIDE, the threat-identification method in Section 5, is applied directly against the entities, processes, data stores, and dataflows on this diagram. A rough DFD now is far cheaper than reconstructing one later from memory.

### 4. Interoperability

- ☐ If your app will ever sync with a third-party platform, such as Apple Health, a provider portal, or an EHR, add that connection to your DFD as a new external entity, even if it is still a future feature.
- ☐ Note what data would cross that connection in each direction, and whether a compromise on either side could affect the other: a corrupted reading flowing into a provider's EHR, or a compromised third-party platform feeding bad data back into your app.
- ☐ Note which data exchange standard you would use (for example, HL7, FHIR, or a vendor-specific API); that choice carries its own security expectations.

Why this matters. The FDA treats interoperability as its own risk category, distinct from general connectivity, with two dedicated deliverables in the full premarket package (Interoperability Risk Assessment and Interoperability Labeling). A compromise does not have to stay on your device; it can travel through an interoperable connection into a hospital's systems, or the reverse.

## 5. Early Threat Identification (STRIDE and CIA)

- ☐ Apply STRIDE to your DFD from Section 3: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. For each process, data store, dataflow, and external entity, note which of the six could apply. Capturing a threat matters more than getting the category exactly right.
- ☐ For each threat you note, tag which of confidentiality, integrity, or availability it threatens. This is the same lens used later for attack-tree analysis on your highest-priority threats.
- ☐ Keep classification separate from scoring. STRIDE says what kind of threat it is; it does not say how bad it is. The formal process scores exploitability, how easy the threat is to carry out, on one axis, and patient harm severity, owned by your team under ISO 14971, on a separate axis. Don't let how-easy-to-attack reasoning creep into a harm judgment, or the reverse.
- ☐ Where a threat could trigger one of the hazards from your Section 2 hazard list, flag it. That link is exactly what the formal threat model and risk assessment will trace in detail.

Why this matters. Our house method uses STRIDE to classify, a CVSS-based exploitability rubric to score, and ISO 14971 for severity, three separate judgments, not one blended score. This follows the MITRE/MDIC Playbook for Threat Modeling Medical Devices, which the FDA itself calls out as the reference standard for this process, not a Blue Goat preference. The sections that follow are your early answer to the next question, what are we going to do about it; keeping threat identification separate from, and ahead of, those controls means your early list maps cleanly onto the formal methodology instead of needing to be redone.

## 6. Authentication, Authorization, and Access Control

- ☐ Confirm how a user's identity is established on the mobile application and the associated cloud account (authentication).
- ☐ Separately, decide what each authenticated role or account is actually allowed to view, change, or delete (authorization). Authentication and authorization are different controls and the FDA expects both addressed.
- ☐ Confirm whether the wearable authenticates the app it pairs with, and vice versa, particularly over Bluetooth.
- ☐ Plan for unique credentials or keys per device or account. Avoid shared or hardcoded defaults.
- ☐ Plan for automatic logoff or a session timeout on the mobile application, so an unattended phone doesn't leave an account open.

## 7. Data Protection and Integrity

- ☐ Confirm encryption in transit between the wearable, the mobile application, and the cloud.
- ☐ Confirm encryption at rest for stored health data.
- ☐ Identify what data qualifies as protected health information and handle it distinctly from wellness or non-regulated data.
- ☐ Plan for how you will detect whether stored or transmitted data has been altered or corrupted (integrity), not only whether it was read by someone unauthorized (confidentiality). These are separate controls in FDA's framework.

## 8. Code and Firmware Integrity

- ☐ Plan to authenticate firmware and software before it runs: verify a digital signature or similar authentication tag before accepting an update or booting, not only when it is first installed.
- ☐ Plan for secure boot, so the device only starts up using software you have verified, not whatever happens to be on it.
- ☐ Disable or restrict test and debug ports, such as JTAG or UART, before the device ships. These are commonly left open on prototypes and forgotten.
- ☐ If the device has a physical enclosure, consider tamper-evident seals so physical tampering leaves visible evidence.

Why this matters. This is a different control than the data integrity question in Section 7: data integrity asks whether your health readings have been altered; code integrity asks whether the software producing those readings is the software you actually built. FDA's guidance treats them as separate, and a device that encrypts its data perfectly while booting unverified firmware still has a meaningful gap.

## 9. Logging and Monitoring

- ☐ Decide what security-relevant events the app and cloud will log: logins, failed login attempts, pairing attempts, configuration changes, and access to health data.
- ☐ Plan for how those logs are protected from tampering and how long they are retained.
- ☐ Confirm logs would be available to support an investigation if a security incident occurred, without exposing more patient data than necessary.

## 10. Resiliency, Recovery, and Disposal

- ☐ Plan for what the device and app do if connectivity, the cloud, or a component fails: does the device fail safely, or does it keep operating on stored data?
- ☐ Plan for backup and recovery of cloud-stored health data.
- ☐ Think about how device and account data will be wiped if a unit is lost, returned, or decommissioned. FDA's recommended approach addresses security through the device's full lifecycle, from initial design through disposal, not only while it is in active use.

## 11. Updatability and Patchability

- ☐ Decide, even at a high level, how firmware and software updates will be delivered and verified, including protection against rollback to an older, vulnerable version.
- ☐ Document your plan for how long components will keep receiving security updates after launch.

## 12. Vulnerability Handling and Disclosure

- ☐ Decide, even informally, how a security researcher or user could report a suspected vulnerability to you.
- ☐ Start a simple internal process for logging and tracking any reported issue; a shared inbox and a spreadsheet are enough at this stage.

- ☐ Know that the FDA requires a formal coordinated vulnerability disclosure process and a postmarket vulnerability monitoring plan in a premarket submission. Building the habit of tracking reports now makes that plan far easier to write later.

## 13. Vulnerability Monitoring

- ☐ Keep a simple list of the third-party components and libraries you are using, the same list you started in Section 3, and periodically check whether any have known vulnerabilities, for example through the National Vulnerability Database (NVD) or CISA's Known Exploited Vulnerabilities (KEV) catalog.
- ☐ This is different from Section 12: that section covers someone reporting a new issue to you; this section covers checking whether issues are already publicly known about what you are already using.
- ☐ When you adopt a new component, check it against those sources once, and note the date you checked, so you have a record to build on later.

Why this matters. The FDA expects premarket submissions to identify all known vulnerabilities associated with the device and its software components, including anything listed in CISA's KEV catalog, and to assess the safety and security risk of each one. Starting this habit with your first few components is far easier than compiling it retroactively against a long component list later.

## 14. Looking Ahead to FDA Premarket Cybersecurity

- ☐ Track design decisions and the reasoning behind them as you make them, so they carry into your formal threat model and risk assessment later. This is the start of operating inside the SPDF described above, well before the formal documentation begins.
- ☐ Know that cybersecurity labeling and a Manufacturer Disclosure Statement for Medical Device Security (MDS2) will eventually be expected. The access-control, logging, backup, and disposal questions above are exactly what those documents ask you to describe.
- ☐ Know that your hazard list, DFD, and threat list above are the seeds of the traceability spine, threat leads to control leads to test leads to patient harm, that anchors the formal premarket package.
- ☐ Plan to begin dedicated cybersecurity documentation and testing once your hardware and software design are stable and market viability is established, rather than on the prototype itself.
- ☐ Revisit this checklist whenever a major design decision changes: cloud provider, connectivity method, or the boundary between the medical and non-medical functions.

*Standards this checklist draws on: FDA Premarket Cybersecurity Guidance (February 2026), Section 524B of the FD&C Act, ISO 14971, ANSI/AAMI SW96:2023, the MITRE/MDIC Playbook for Threat Modeling Medical Devices, and DFD3 (Shostack). Not house preference; these are the standards the formal engagement rests on.*



Ready to talk through where you stand, or want help with any item above?

**Scan to book a discovery session with Blue Goat Cyber.**

[go.bluegoatcyber.com/meetings/blue-goat-cyber/discovery-session](https://go.bluegoatcyber.com/meetings/blue-goat-cyber/discovery-session)