Medical Device Cybersecurity Checklist

Brought to you by Block Harbor

Checklist Question	Score (0/0.5/1)	weight (1,2,3)
1. Asset & System Definition		
Have we identified all device assets (hardware, firmware, software, APIs, cloud services, mobile apps)?		
Have we documented all data flows (PHI, telemetry, commands)?		
Have we defined intended use & critical clinical functions?		
Have we listed all connectivity interfaces (Wi-Fi, Bluetooth, USB, hospital LAN, cellular)?		
2. Cybersecurity Goals		
Have we defined goals for **patient safety** (device must not cause harm if attacked)?		
Have we defined goals for **data privacy** (PHI must not be leaked or altered)?		
Have we defined goals for **system reliability & availability** (device must operate during cyber events)?		
Have we tied goals to measurable requirements (e.g., uptime ≥ 99.9%, AES-256 for PHI)?		
3. FDA Premarket Guidance		
Has a **Threat Modeling / TARA** been performed?		
Do we maintain a **Cybersecurity Risk Management Plan**?		
Do we provide a **SBOM** for all third-party & OSS components?		

Does the device have a **secure update mechanism** (cryptographic signing, rollback protection)?		
Have we done **security testing** (penetration testing, fuzzing, vulnerability scans)?		
Is there a defined **post-market monitoring & incident response plan**?		
4. HIPAA Privacy & Security Rule		
Is PHI encrypted **in transit** (TLS 1.2+)?		
Is PHI encrypted **at rest** (AES-256 or equivalent)?		
Are **access controls** in place (RBAC, MFA, least privilege)?		
Are **audit logs** generated for all PHI access and protected from tampering?		
Is there a documented **breach notification process**?		
5. ISO 14971 Risk Management		
Have cybersecurity hazards been identified (e.g., incorrect therapy, loss of monitoring, denial of service)?		
Have risks been linked to **patient safety outcomes**?		
Have controls been applied & their effectiveness verified?		
Is there a **traceability chain** hazard → risk → control → test?		
6. IEC 62304 Software Lifecycle		
Are secure coding guidelines applied (input validation, memory safety, crypto use)?		
Is there **version control and change management** for all software/firmware?		
Are all software requirements and test cases documented?		
Has **software risk analysis** included cybersecurity threats?		
Is there a formal **patch & update policy** for fielded devices?		

7. Structured Risk Assessment (TARA Principles)		
Are assets, threats, feasibility, and impacts clearly defined?		
Are risks **prioritized** with treatment decisions (mitigate, accept, transfer, avoid)?		
Is TARA **re-run** after design changes or new vulnerabilities?		
Are **lessons learned** reused across device families?		
Do we maintain **continuous monitoring of emerging threats**?		

Scoring System

Each checklist item is scored:

- **0 = Not addressed**
- **0.5 = Partially addressed**
- **1 = Fully addressed with evidence**

Because not all items are equally critical, each one also has a **weight**:

- **3 = High-criticality** (e.g., encryption, secure updates, incident response, SBOM)
- **2 = Medium-criticality** (e.g., asset inventory, risk management, software lifecycle)
- **1 = Low-criticality** (e.g., lessons learned, documentation reuse)

Your **final score** is calculated as:

$$\text{Final Score} = \frac{(\text{Score} \times \text{Weight for all items})}{\text{Maximum Possible Score}} \times 100$$

How to Interpret Results

- **85–100% → Secure & Audit-Ready**
- **70–84% → Mostly secure, gaps need closure**
- **50–69% → Weak security, high audit risk**
- **Below 50% → Not secure / not compliant**