What Investors and Hospital Audit Before Approval?

Prepare a security pack containing all of the following requirements that helps you enter any hospital pilot conversation.

Data Architecture

- Is ePHI clearly isolated from other system data?
- Is encryption in place at rest and in transit?
- Is data residency appropriate for the target market?

Access Controls

- Is MFA enforced across all environments?
- Is role-based access control implemented and documented?
- Are privileged access logs available and tamper-protected?

IEC 62304 and SaMD

- Does the development process conform to IEC 62304 for any SaMD components?
- Is there a software safety classification rationale documented?
- Is there a complete risk management file per ISO 14971?

Vendor and Third-Party Risk

- Are BAAs in place with every vendor that touches ePHI?
- Have vendors been assessed for security compliance, not just asked to self-certify?

Incident Response

- Is there a documented incident response plan?
- Has it been tested? When?
- What is the breach notification workflow and timeline?

SOC 2 Status

- Has a SOC 2 Type II audit been completed or is one in progress?
- What trust service criteria are in scope?

Hospital Procurement Security Review

Hospital IT security teams in 2026 consistently request:

- Penetration test results within the last 12 months
- SOC 2 Type II report (standard at most US health systems above 200 beds)
- Business Continuity and Disaster Recovery plan with tested Recovery Time Objectives
- Data Flow Diagram showing exactly where PHI travels through your system
- Subprocessor list with BAA confirmation for each
- IEC 62304 conformance documentation (for any SaMD component)
- Employee security training records

Checking the boxes is only 20% of the battle; **Book a 1: 1 Strategy Call** to learn how to prove the other 80% to even the most cynical hospital auditor.

Not ready for a 1:1? Read this guide on your product's tech due diligence for Series A.