CHECKLIST

Medical Device Cybersecurity Vendor Evaluation Checklist

20 questions to ask before you sign - separates real MedTech specialists from generalists

Most cybersecurity vendors will tell you they 'do' medical devices. Few have ever actually shipped one through FDA. Use these questions in your next vendor conversation; the answers reveal more than any case study.

MedTech-specific experience

- [ ] How many 510(k) / De Novo / PMA submissions has your team supported in the last 24 months?
- [ ] Can you name a recent FDA AI request you helped resolve, and what the deficiency was?
- [ ] Who on your bench has authored or contributed to an SBOM accepted by FDA?
- [ ] What is your stance on the February 2026 final premarket guidance - what changed for you?

Pen-testing methodology

- [ ] Do you test against the physical device, the cloud companion app, AND the firmware update path?
- [ ] What does your hardware bench look like - JTAG, glitchers, logic analyzers, RF tooling?
- [ ] Will you provide a sanitized sample report from a comparable device class?
- [ ] How do you scope re-test cycles after we remediate findings?

Threat modeling depth

- [ ] Which framework do you use (STRIDE, PASTA, MITRE/MDIC playbook, hybrid)?
- [ ] How are trust boundaries documented and traced into the security risk file?
- [ ] Do you produce threat models reviewers can read, or developer-only artifacts?

Engagement & commercials

- [ ] Is the named senior consultant you pitch the same person who will run my engagement?
- [ ] What is your typical turnaround for an AI-request response?
- [ ] Are deliverables priced per submission, per quarter, or hourly - and why?
- [ ] What happens if FDA comes back with follow-up questions after delivery?

Red flags to disqualify

- [ ] They cannot name a specific reviewer interaction or guidance they've operationalized.
- [ ] Their pen-test 'methodology' is a copy of OWASP Top 10 with no hardware coverage.
- [ ] Threat modeling is delegated to a junior or entirely automated.
- [ ] Pricing is opaque or shifts dramatically once scope is shared.

Ready to talk through your roadmap?

Book a Strategy Session →