MEDICAL DEVICES

Medical Device Security Assessment

Penetration testing, post-quantum readiness and AI security for connected medical devices — premarket evidence for manufacturers, and fleet assessments for the hospitals that run them.

FDA
REPORT-READY

Bench-only
NEVER ON A PATIENT

CycloneDX
CBOM & ML-BOM OUTPUT

Senior
PRACTITIONER-LED

What we assess

AI security

AI-enabled device software, training-data provenance, controlled model updates, and assistants that can reach patient data.

Post-quantum readiness

Firmware and update signing, device identity certificates, and the links carrying patient data that must stay confidential for decades.

Device & ecosystem testing

The device on the bench, its wireless and telemetry links, companion app, cloud and update infrastructure, and the clinical interfaces it speaks.

What you get

- ✓ Pen test report built to FDA's named elements, with your disposition of each finding
- ✓ Fleet assessment for providers: inventory, segmentation, legacy exposure
- ✓ Access-control advice checked against emergency clinical access
- ✓ Patient-harm findings escalated the moment we find them
- ✓ CBOM and a post-quantum roadmap for your device service lives
- ✓ AI Bill of Materials (AI-BOM) in CycloneDX ML-BOM format
- ✓ One round of retesting to confirm the fixes landed

How it works

1. Scope against the device, its intended use, and target markets
2. Agree the safety gate and the test units before any work starts
3. Test bench units hands-on; passive-only discovery on hospital networks
4. Deliver evidence and findings, then retest the fixes

A good fit if

- ✓ You are preparing an FDA premarket submission and need a pen test report a reviewer can rely on.
- ✓ Your notified body is asking how your device meets the state of the art for security.
- ✓ You run a fleet of connected devices you did not build and cannot easily patch.
- ✓ Your devices stay in service for years, and their keys and patient data must stay protected that long.

Probably not, if

- ✗ You want devices in clinical use tested — we never test a device connected to a patient.
- ✗ You need clearance or a CE certificate — we produce the evidence; FDA and your notified body decide.
- ✗ You want clause-by-clause claims against standards we have not licensed — we quote only what we have read.

How we engage

Fixed scope
A fixed-scope proposal at a fixed price. No hourly meter running.

Senior-led
The practitioner who scopes the work does the work and writes the report.

Plain language
One report your engineers and your board can both act on.

Patient safety first
Never on a patient, therapy functions on simulators only, licensed RF only.

Security that locks down risk, not your business. · © 2026 verrou