IBLADES WHITEPAPER · HEALTHCARE & LIFE SCIENCES

Quantum-Resilient Security for Connected Care

Protecting connected medical devices, health information exchange, and lifetime patient data against quantum and AI-era threats — without disrupting patient care.

← Healthcare & Life Sciences

In this paper

1. Executive summary

Healthcare is undergoing rapid digital transformation, driven by the integration of artificial intelligence, the Internet of Medical Things (IoMT), and unified health information exchanges that connect hospitals, clinics, and care networks. While these advancements improve patient outcomes, they expose the sector to two critical risks: an "unpatchable" edge of legacy connected medical devices that cannot be secured with traditional software agents, and a "harvest now" threat against patient and genomic data that must remain private for a lifetime.

iBlades secures this environment with a single, hardware-anchored, post-quantum security fabric that overlays existing clinical and IT infrastructure. It isolates vulnerable

medical devices without disconnecting them from care, protects data in transit against future quantum decryption, and counters AI-driven attacks by shrinking the exposed software surface — all without changes to clinical applications or medical device certifications.

---

2. The 2026 threat landscape

The "unpatchable edge" of legacy medical devices

Hospitals and health systems are filled with expensive, long-lived connected medical devices — imaging systems, infusion pumps, monitors, and diagnostic consoles — that run outdated operating systems and cannot be patched without voiding manufacturer warranties. These devices become open doors for ransomware, which moves laterally from a compromised administrative PC toward life-support and other critical clinical systems.

AI-accelerated attacks

AI-powered attacks run at machine speed — discovering vulnerabilities in minutes, probing thousands of connected endpoints at once, generating evasive malware, and mapping trust relationships to move laterally after a foothold. Against AI-driven clinical and diagnostic systems, **data poisoning** (spoofed telemetry or sensor feeds) becomes a patient-safety concern, not just a data concern.

> **The real target is complexity.** AI attacks feed on exposed APIs, admin consoles, agents, and remote-access paths. Reducing that software surface does more to stop them than adding another software layer.

Harvest Now, Decrypt Later (HNDL)

Adversaries capture encrypted patient and genomic data today to decrypt it once quantum computers mature. Healthcare is uniquely exposed: unlike a credit card number, a patient's genomic profile or medical history cannot be reissued after a breach, and health records must remain confidential for a lifetime — making healthcare data an especially severe target for the "harvest now, decrypt later" strategy.

3. The iBlades architecture

One hardware-anchored, quantum-ready fabric, built on NIST-standardized post-quantum cryptography (ML-KEM for key exchange, ML-DSA/Dilithium for signatures; FIPS 203/204) with keys generated locally and rotated autonomously.

- **GuardTron™** — an agentless "digital quarantine" for connected medical devices. Plug a legacy imaging system, infusion pump, or monitor into GuardTron and it is instantly isolated from the general network ("invisible" to ransomware scanners) while keeping a secure, encrypted tunnel to the specific systems it needs to talk to. No software agent is installed on the device, so manufacturer warranties and certifications remain intact.
- **NetTron™** — a software-defined, peer-to-peer quantum-safe mesh that moves data between facilities, clinics, and health information exchanges. It uses NIST post-quantum algorithms with autonomous key rotation every 60–300 seconds, so an intercepted session yields only seconds of useless data, and cryptographically signs data flows to prevent tampering.
- **ManoTron™** — hardware-secured mobile communications for telemedicine and clinician mobility, routing traffic through a secure, encrypted tunnel that bypasses the vulnerabilities of home Wi-Fi and public cellular networks.

AI-resilient by design

- **Reduced attack surface** — fewer exposed interfaces and agents for AI to probe.
- **Hardware-anchored trust** — trust in dedicated hardware that can't be scanned or manipulated like software.
- **Cryptographic isolation** — blocks AI-driven lateral movement even after a compromise, keeping breaches on the IT network from reaching connected medical devices.
- **Works alongside your stack** — inline and transparent; complements existing firewalls, EDR/XDR, SASE, and identity tools.

4. Regulatory & compliance mapping

Framework	Requirement	How iBlades enables it
NIST PQC (FIPS 203/204)	Migration to quantum-safe algorithms	Native ML-KEM / ML-DSA across NetTron and GuardTron
HIPAA	Safeguard the confidentiality, integrity, and availability of protected health information	PQC encryption in transit, hardware isolation of vulnerable devices, immutable audit logging
ISO 27001	Information security management system controls	Zero-trust access, encrypted device tunnels, continuous audit trails
IEC 62443	Security for operational technology, including connected medical devices	GuardTron hardware isolation of legacy devices without software agents
National health data-protection standards	Medical device security, access control, and audit requirements common across health-sector regulation	Device isolation, identity-based zero-trust access, immutable logging, and on-premise/sovereign routing options

---

5. A low-risk pilot path

- **Select** a handful of high-risk, legacy connected medical devices that cannot be patched (for example, an imaging console or a diagnostic system).
- **Deploy** GuardTron nodes in bridge mode in front of these assets — a fast install with no changes to clinical applications or device configuration.
- **Validate** isolation with a penetration test; the devices become invisible to network scanners while retaining full connectivity to the systems they depend on.
- **Demonstrate** post-quantum key rotation and audit evidence for the security and compliance team; reverse cleanly if desired.

Ready to secure your connected care environment?

Request a briefing to see how a low-risk pilot would work in your environment.

Request a briefing

⬇ Download PDF

Back to overview

Prefer email? Reach us at hello@iblades.ai

---

iblades.ai™
safe. effective. secure.

Safe, effective, secure.

Next-generation cyber architecture making cybersecurity simple, reliable, and accessible for everyone.

hello@iblades.ai

Products

- NetTron™
- GuardTron™
- ManoTron™
- Pricing

Solutions

- Financial Institutions
- Healthcare
- Infrastructure
- Government & Military

Company

- About Us
- Partners
- Documentation
- Contact

Compliance

- NIST Approved
- SOC 2 Type II
- HIPAA Compliant
- ISO 27001
- FedRAMP Ready

HEADQUARTERS
127 Spring Street, Suite 120
Pleasanton, CA 94566

R&D CENTER
795 24th Street
Ogden, UT 84401