DATA SHEET

Securing Healthcare Networks and Medical Devices with Terniion™

The Problem: Clinical Uptime Meets Escalating Cyber Risk

Healthcare runs on aging infrastructure, vulnerable medical devices, and an ever-expanding web of cloud services, clinics, and partners. Large breaches and ransomware are rising, and a single incident can disrupt patient care, trigger regulatory penalties, and damage trust.

The constraints are tough:

- Legacy imaging, lab, and bedside devices run aging operating systems that cannot easily be patched or replaced.
- Clinical teams depend on remote access tools and VPNs that create standing entry points into sensitive environments.
- PHI, EHRs, and critical apps are spread across on-prem, cloud, and third-party systems, all under strict compliance pressure.

Traditional perimeter and VPN approaches were not built for this mix of fragile devices and always-on care. If a clinical system can be scanned or directly addressed over the network, it is vulnerable to attack.

Terniion eliminates attack surfaces across healthcare networks and medical devices without forcing rip-and-replace or clinical downtime.

Business Outcomes for Healthcare

Reduced Risk to Patient Safety and Care Disruption

Non-routable networks and process-level isolation reduce the blast radius to dramatically lower the chance that a cyber incident takes down EHRs, imaging systems, bedside devices, and other critical infrastructure during critical care windows.

Less Operational Complexity

Closing inbound ports, eliminating legacy VPN dependencies, and using one overlay for hospitals, clinics, and medical IoT simplifies architectures and reduces brittle firewall and remote-access configurations.

Lower Cost of Compliance and Control

Fewer security point tools and less emergency patching around exposed systems reduce both security spend and compliance overhead.

Modern Security Without Replacing Medical Devices

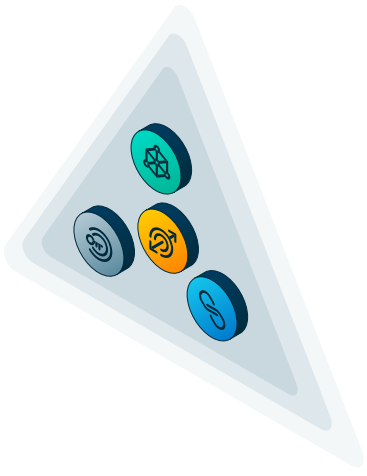
Terniion wraps vulnerable medical and IoT devices like those used in imaging, monitoring, lab, and building systems, without firmware changes or costly device swaps, extending secure lifespans and protecting capital investments.

5 Best Practices for Securing Healthcare Infrastructure

Best Practice	Key Actions	Xiid Terniion Solution
Protect Unpatchable and Legacy Medical Devices	Accept that many imaging, monitoring, and diagnostic systems cannot be frequently patched or replaced.	Terniion overlays existing devices as-is. Systems operate behind closed inbound ports while remaining fully usable for clinicians.
Make Clinical Systems and PHI Stores Non-Routable	Prevent direct internet or partner access to EHRs, PACS, LIS/RIS, and other core clinical apps.	SealedTunnel technology makes clinical applications and data stores non-addressable from external networks. Access only flows through outbound-only, triple-encrypted, process-to-process tunnels.
Secure Remote Access for Clinicians and Staff	Replace broad VPNs and exposed remote desktop/jump hosts with scoped, safer access.	Clinicians, IT, and vendors connect via process-bound tunnels that grant access only to specific applications, not the entire network. VPN requirements and risks shrink.
Contain Insider and Lateral Movement Risk	Assume some endpoints will be compromised; prevent spread to critical systems.	Lateral movement is structurally prevented. Process-level microsegmentation ensures that compromise of a workstation or device cannot pivot into EHRs, directory services, or high-value clinical systems.
Future-Proof PHI and Clinical Data in Transit	Plan for “harvest-now, decrypt-later” threats against long-lived PHI and clinical telemetry.	Triple-layer, quantum-resistant encryption protects PHI, imaging data, and clinical workflows in transit even against adversaries who plan to decrypt captured traffic years from now.

Key Components

- **SealedTunnel**
  Executed via STLink— a lightweight software agent on either end, these are outbound-only, triple-encrypted, process-to-process tunnels that perform reliably even over unstable networks, ideal for distributed clinical sites.
- **Commander**
  The control brain coordinating secure connections across cloud, on-prem, and hybrid environments. It centralizes policy so "who can talk to what" becomes maintainable rules instead of 10,000 firewall exceptions.
- **Connector**
  Joins two outbound-only communication halves without ever decrypting traffic. It serves as a secure rendezvous where quantum-encrypted messages are dropped off and picked up by authorized STLinks, keeping critical infrastructure undiscoverable.
- **Aclave**
  Credential-less authentication that lets staff and partners access systems without usernames, passwords or long-lived credentials.



How Terniion Secures Healthcare Environments

Terniion enables clinical systems to operate with no inbound exposure. It is a secure network access control platform that acts as an overlay across hospitals, clinics, data centers, and cloud workloads.

Clinical Applications and PHI Systems

- EHRs, EMRs, PACS, LIS/RIS, and billing systems operate with all inbound ports closed.
- Only authenticated, policy-approved processes can reach them via outbound-only, process-to-process tunnels.
- Attackers cannot scan or directly connect to these systems over the network.

Medical Devices and Clinical IoT

- Imaging systems, infusion pumps, monitors, microscopes, DICOM/PACS clients, and other devices remain deployed as-is.
- Terniion places their communications behind outbound-only SealedTunnel connections, closing inbound ports and making them unreachable to external attackers.
- Even if device software is outdated and vulnerable, malicious actors are left with virtually no exposed attack surface with which to exploit them.

Clinician, Staff, and Vendor Access

- Clinicians access remote desktops, clinical apps, and imaging systems without starting traditional VPN sessions or exposing RDP/VDI gateways.
- Field staff, biomedical engineers, and vendors receive tightly scoped access to specific systems, for specific purposes, over encrypted tunnels.
- A compromised vendor account can no longer traverse into the broader hospital network.

High-Value Healthcare Use Cases

- **Securing Vulnerable Medical Devices and Imaging Systems**
  Legacy MRI, CT, X-ray, and lab systems often run outdated and vulnerable software but are mission-critical. Terniion allows care to continue unchanged while removing direct network exposure and wrapping device traffic in triple-layer encryption.
- **Protecting EHRs and Clinical Workflows from Ransomware**
  System Intrusion attacks increasingly target healthcare, often via stolen credentials and exposed services. With Terniion, EHRs and supporting databases are non-routable, and process-level isolation makes lateral movement into these systems far more difficult.
- **Remote Access for Nurses, Clinicians, and Telehealth**
  Nurses, physicians, and remote clinicians can access critical apps and desktops securely from clinics, home, or temporary sites without opening new VPN concentrators or exposing RDP/VDI endpoints.
- **Multi-Site and Partner Connectivity**
  Hospitals, clinics, imaging centers, and third-party service providers connect over outbound-only tunnels. Each site or partner gets a defined access pattern, rather than permanent network-level trust.

FAQS

Will this require replacing existing medical devices or disrupting clinical workflows?

No. Terniion is designed as an overlay. It wraps existing devices and applications without requiring firmware changes, device swaps, or major workflow redesign, and can be phased in starting with the highest-risk systems.

How does Terniion interact with our current VPN, ZTNA, and identity tools?

Terniion sits alongside your existing stack. It reduces dependence on VPNs for clinical access and extends strong, process-level controls behind your ZTNA and identity layers, streamlining complex security stacks over time without requiring rip-and-replace.

What does this mean for HIPAA and other regulatory expectations?

By closing inbound ports, tightening access around PHI systems, and securing data in transit with strong, future-conscious encryption, Terniion supports a more defensible posture for regulators, auditors, and insurers.

The Bottom Line

Healthcare can't secure its systems by patching faster or adding more firewall rules. The only truly secure way forward is to eliminate exposure by design. **Terniion gives you a way to:**

- Protect vulnerable medical devices and clinical systems without replacing them.
- Reduce the likelihood that cyber incidents disrupt patient care.
- Simplify a complex remote-access and security stack.
- Strengthen compliance posture while controlling cost and operational drag.

Secure the systems your clinicians—and patients—depend on, without sacrificing availability.

Ready to see how this works across your hospitals, clinics, and device fleets?
Read more about Terniion | See a live demo