ChiefNET

CHIEFNET OT SHIELD · USE CASE

Securing Healthcare & Hospital Networks

Unidirectional Data Transfer for Medical Devices, Clinical Systems and Hospital IT

Hospitals · Health Systems · Clinical

Document reference	Version	Date	Published by
CN/OTS/UC/HEALTHCARE/v1.0	1.0	June 2026	ChiefNET Private Limited

Contents

1. Executive Summary
2. Industry Context: Cybersecurity Challenges in Healthcare
3. ChiefNET OT Shield: Solution Overview
4. Reference Architecture
5. Detailed Use Cases
6. Compliance & Standards Alignment
7. Business Value
8. ChiefNET OT Shield vs. Traditional Firewalls
9. Technical Capability Snapshot
10. Deployment & Engagement Model
11. Conclusion

Also available online at chiefnet.io/use-cases/ot-shield/healthcare/

Executive Summary

Hospitals and healthcare networks depend on an expanding universe of connected medical devices – patient monitors, infusion pumps, imaging systems and other Internet of Medical Things (IoMT) equipment – that were engineered for clinical reliability, not for resisting network intrusion. As health systems adopt electronic health records, cloud analytics and remote patient monitoring, every new connection between the clinical network and hospital IT becomes a potential path for ransomware or data theft, at a time when a compromised clinical device can directly endanger patient safety.

ChiefNET OT Shield is a hardware-enforced data diode purpose-built to close that gap. It allows patient monitor data, imaging metadata, device telemetry and facility system data to flow out of the clinical network to the hospital's EHR, analytics and cloud systems, while making it physically impossible for any command, malware or intrusion attempt to flow back in. There is no firewall rule to misconfigure and no firmware to patch on life-critical clinical equipment; isolation is built into the hardware itself.

This document presents a use-case-driven view of how ChiefNET OT Shield applies to healthcare environments – covering reference architecture, detailed use cases, regulatory alignment, and the business case for deployment across hospitals, clinics and diagnostic centres.

> **Why this matters for healthcare providers**
>
> Ransomware attacks on hospitals have repeatedly forced emergency departments to divert patients and clinical systems to fail over to manual processes. A hardware-enforced one-way data path removes the most common route ransomware uses to reach clinical devices from a compromised hospital IT network.

Industry Context: Cybersecurity Challenges in Healthcare

A Sector Racing to Digitise Patient Care

Health systems are connecting an ever-growing range of medical devices and clinical systems to hospital networks in pursuit of better outcomes: remote patient monitoring, AI-assisted diagnostics, centralised imaging archives and population health analytics all depend on data flowing out of clinical devices and into hospital IT and cloud platforms. In many hospitals, this connectivity has been added incrementally on top of flat clinical networks, so a breach anywhere on the hospital IT side can reach connected medical devices directly.

A Well-Documented Threat History

Healthcare has become one of the most heavily targeted sectors for ransomware precisely because outages are so costly – hospitals under attack have had to cancel surgeries, divert ambulances and revert to paper records. The 2017 WannaCry ransomware outbreak notably disrupted hospital

operations at UK National Health Service trusts by spreading through unpatched Windows systems on hospital networks, including systems connected to medical equipment. Since then, hospital ransomware incidents have continued at a steady pace globally, frequently entering through a compromised IT endpoint or third-party vendor connection before spreading towards clinical systems.

Why General-Purpose IT Security Falls Short

- Firewalls and VPNs are software-defined and bidirectional by design – a misconfigured rule, an unpatched CVE, or a stolen credential can open a path back into the clinical network.
- Medical devices often run on long product lifecycles with limited or no ability to install security patches, since patching requires re-validation of regulated equipment.
- Many hospitals operate flat clinical networks where a single compromised device or endpoint can potentially reach other connected medical equipment.
- IT and clinical engineering teams are often separately resourced, making end-to-end network segmentation difficult to design and enforce consistently.

Regulatory and Standards Drivers

Healthcare providers operate under explicit data protection and patient safety obligations that increasingly reference network segmentation as an expected control:

- **HIPAA Security Rule (where applicable):** requires technical safeguards to protect the confidentiality, integrity and availability of electronic protected health information, including access and transmission controls.
- **Ayushman Bharat Digital Mission (ABDM) Guidelines, India:** set data security and interoperability expectations for health data flowing between facilities and the national digital health ecosystem.
- **ISO 27799 (Health Informatics Security):** provides sector-specific guidance for applying information security management to health information, including network segmentation between clinical and administrative systems.
- **CERT-In & Sectoral Health CERT Advisories (India):** reinforce baseline security hygiene and incident-reporting obligations for healthcare and critical information infrastructure.
- **Medical Device Cybersecurity Guidance:** regulators increasingly expect connected medical devices to be deployed within segmented network architectures rather than relying solely on device-level security.

ChiefNET OT Shield: Solution Overview

ChiefNET OT Shield is a purpose-built cybersecurity appliance combining a hardware-enforced data diode with a hardened, cloud-managed communications platform. It is designed to sit precisely at the boundary between the clinical device network and the hospital IT, EHR or cloud systems that

need visibility into it.

Core Architecture

- Physical transmitter (TX) module on the secure/restricted side and a physically separate receiver (RX) module on the monitoring/enterprise side, joined only through an optical, one-way link.
- No physical mechanism exists for signals to travel from the RX side back to the TX side – isolation is enforced by hardware, not by a rule set that can be disabled or bypassed.
- A hardened operating system on both sides minimises attack surface and removes the general-purpose services that create most software vulnerabilities.

Key Capabilities

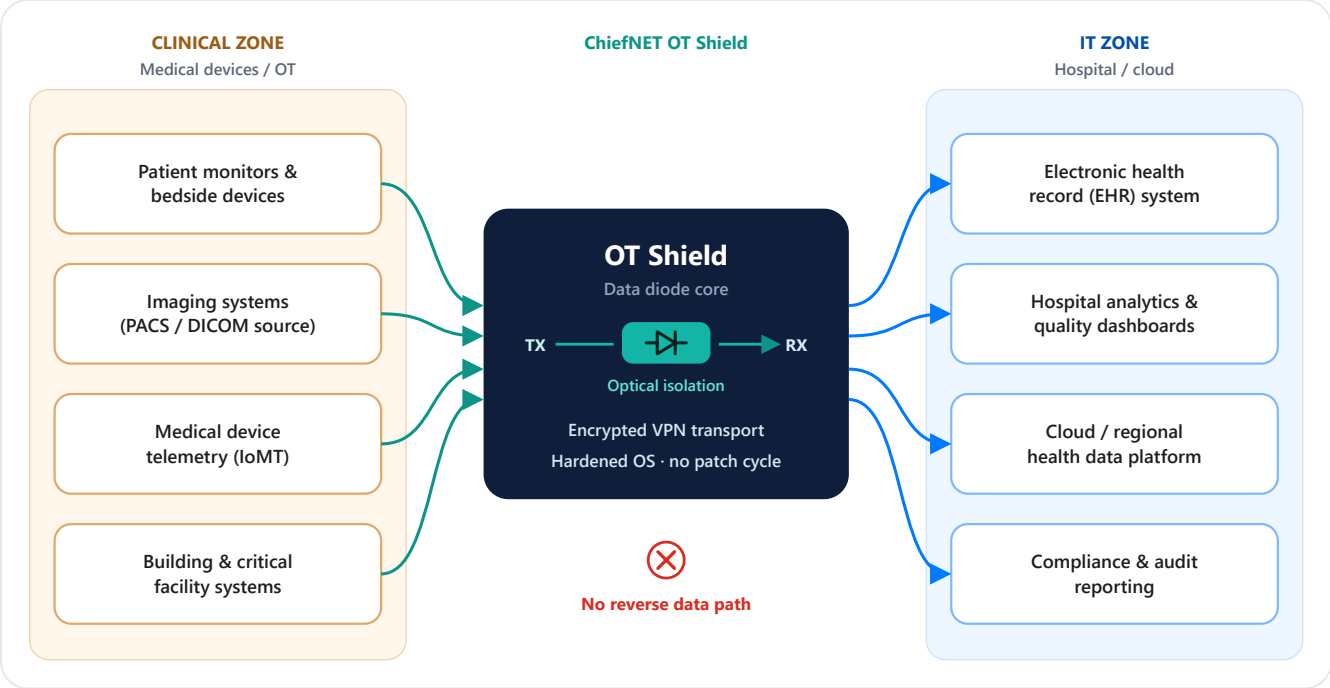
- **Native protocol support:** BACnet, Modbus, MQTT, OPC UA and industrial UDP (broadcast/multicast/anycast), covering medical device telemetry and building/facility automation.
- **File and log transfer:** UDP file transfer, Syslog and HTTP PUT for device logs, imaging metadata exports and facility system events.
- **Encrypted VPN transport:** data exiting the diode is carried to the EHR, analytics platform or cloud endpoint over a hardened, encrypted tunnel, protecting patient data in transit without reopening a return path.
- **Dual WAN / 4G-5G failover:** on the monitoring (RX) side, ensuring uninterrupted delivery of clinical data even where hospital network infrastructure is degraded.
- **Built-in SD-WAN functionality:** for health systems with multiple facilities, enabling secure interconnection of hospitals and clinics with central IT while keeping each facility's clinical network isolated.
- **Centralised cloud orchestration:** zero-touch and pre-provisioning, fleet-wide monitoring, alerting and dashboards – essential for multi-facility health systems.
- **Zero patch burden:** because isolation is physical rather than rule-based, there is no firewall ruleset or reverse-path exploit to patch against – critical for medical devices that cannot be routinely patched.

Reference Architecture

Single-Site Deployment – Hospital / Clinical Network

At a single hospital, ChiefNET OT Shield sits between the clinical zone (patient monitors, imaging systems, medical device telemetry, facility systems) and the IT zone (EHR system, hospital analytics, cloud health platforms, compliance reporting). All operational data leaves the clinical zone through

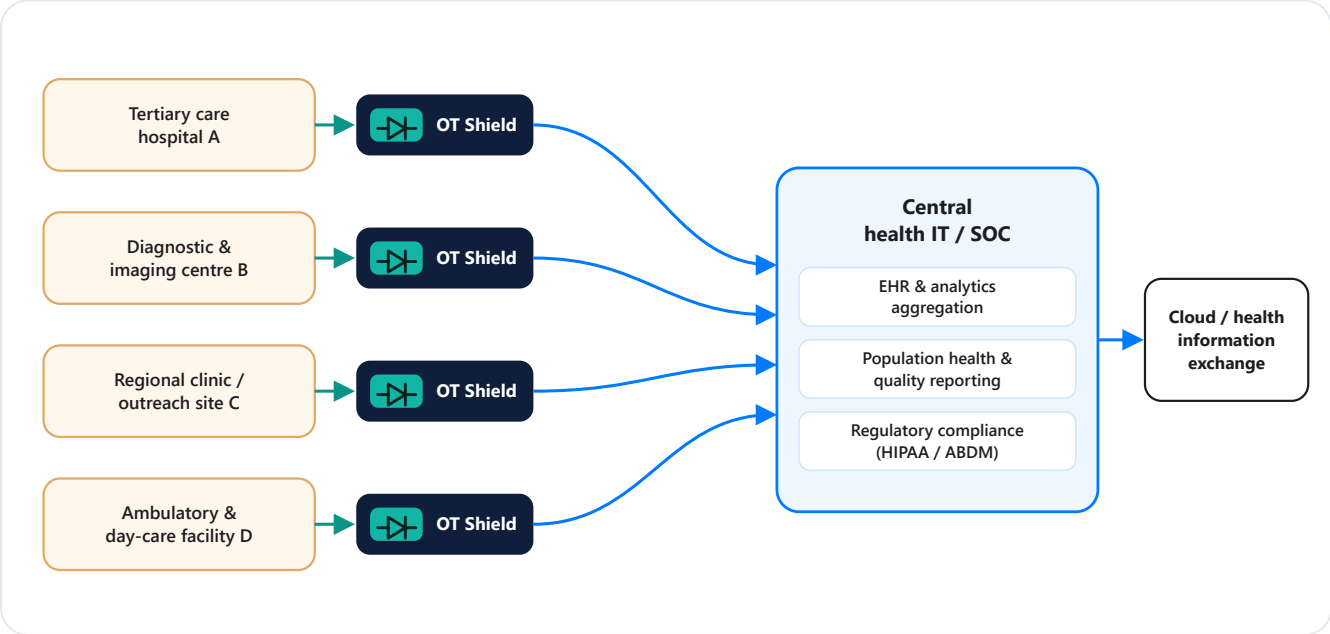
the diode's transmitter; nothing – no command, no query, no malware – can traverse back to a connected medical device.



Single-site reference architecture – unidirectional data flow from clinical/medical device networks to hospital IT

Multi-Facility Deployment Across a Health System

Health systems operating multiple hospitals, diagnostic centres and clinics can deploy one OT Shield per facility, provisioned and monitored from a single cloud console, while each facility's isolation guarantee remains entirely local and independent – a compromise or outage at one facility cannot propagate to another.



Multi-facility deployment – hospitals and clinics converging on a central health IT SOC

Detailed Use Cases

The following use cases illustrate how ChiefNET OT Shield is applied across hospital, clinic and diagnostic environments.

USE CASE 5.1

Patient Monitor & Bedside Device Data Export to EHR

Clinical Networks

Challenge	Clinical teams need patient monitor and bedside device data flowing into the electronic health record for charting and clinical decision support, but the medical device network must remain isolated from hospital IT to protect life-critical equipment.
OT Shield solution	OT Shield taps patient monitor and bedside device telemetry on the secure clinical side and replicates it one-way to the EHR system on the IT side over an encrypted VPN, using OPC UA / MQTT protocol support – with zero possibility of write-back to connected devices.
Outcome	✓ Automated vitals charting without touching the medical device network ✓ Reduced manual data entry and transcription error ✓ Medical device network remains fully isolated from any external network path

USE CASE 5.2

Medical Imaging Metadata & PACS Data Flow

Radiology & Diagnostic Imaging

Challenge	Radiology departments need imaging metadata and study information to flow to enterprise PACS and analytics systems for reporting and AI-assisted diagnostics, without exposing the imaging network to external systems.
OT Shield solution	OT Shield forwards imaging metadata and study information one-way from the imaging network to enterprise PACS and analytics platforms, supporting UDP file transfer for large imaging data sets.
Outcome	✓ Enterprise-wide access to imaging data for reporting and AI analytics ✓ Imaging network isolated from broader hospital and external networks ✓ Supports centralisation of imaging archives across a health system

USE CASE 5.3

Remote Patient Monitoring & IoMT Device Telemetry

Connected Medical Devices (IoMT)

Challenge	Health systems want continuous telemetry from a growing base of connected medical devices for remote monitoring and predictive alerts, but each additional connected device expands the potential attack surface of the clinical network.
OT Shield solution	OT Shield provides a single, hardware-enforced export point for IoMT device telemetry, allowing the fleet of connected medical devices to grow without expanding the network's exposure to inbound threats.
Outcome	✓ Scalable IoMT monitoring without proportionally increasing risk ✓ Single point of hardware-enforced isolation for the whole device fleet ✓ Supports predictive alerting and remote monitoring programmes

USE CASE 5.4

Hospital Facility & Critical Systems Monitoring

Building & Life-Safety Systems

Challenge	Facilities teams need visibility into HVAC, medical gas, power and life-safety systems across a hospital campus, but these systems are safety-critical and must not accept inbound connections from hospital IT.
OT Shield solution	OT Shield exports facility and life-safety system telemetry one-way to a centralised facility management platform, following the same zone/conduit segmentation principles used in critical infrastructure.
Outcome	✓ Centralised facility visibility without exposing life-safety systems ✓ Consistent segmentation approach across hospital campuses ✓ Simplifies compliance with hospital accreditation and safety audits

USE CASE 5.5

Multi-Facility Population Health & Quality Reporting

Health Systems & Hospital Groups

Challenge	Health systems operating multiple hospitals and clinics need to aggregate clinical and quality data centrally for population health analytics and regulatory reporting, without bridging separate facility networks together.
OT Shield solution	Each facility's OT Shield independently isolates its own clinical network while permitting data to be aggregated and cross-analysed at the health system's central IT or cloud layer, so visibility can be pooled without ever connecting two clinical networks directly.
Outcome	✓ System-wide population health visibility without direct network-to-network connectivity ✓ Each facility retains independent, physically enforced isolation ✓ Supports regulatory quality reporting and ABDM-aligned data sharing

USE CASE 5.6

Secure Vendor & Biomedical Engineering Support

Medical Device OEM & Biomedical Support

Challenge	Medical device OEMs and biomedical engineering teams often need diagnostic data from equipment for remote support and preventive maintenance, but granting inbound remote access to clinical device networks raises significant patient safety and security concerns.
OT Shield solution	OT Shield provides OEMs and biomedical engineering platforms with a one-way feed of the diagnostic data needed for remote support, removing the need to grant any inbound remote access into the clinical device network.
Outcome	✓ Vendor and biomedical support enabled without inbound access to clinical devices ✓ Reduces a common root cause of medical-device-linked security incidents ✓ Simplifies vendor access governance and audit for biomedical engineering

Compliance & Standards Alignment

The table below maps ChiefNET OT Shield capabilities to the regulatory and standards expectations most relevant to healthcare providers.

Framework / Requirement	Requirement Summary	How OT Shield Addresses It
HIPAA Security Rule (where applicable)	Technical safeguards to protect confidentiality, integrity and availability of health information.	Hardware data diode enforces one-way transfer, limiting exposure of clinical systems handling protected health information.
Ayushman Bharat Digital Mission (ABDM)	Data security and interoperability expectations for health data exchange.	Enables secure, auditable one-way data export to national/regional digital health platforms.

Framework / Requirement	Requirement Summary	How OT Shield Addresses It
ISO 27799 (Health Informatics Security)	Apply information security management to health information, including network segmentation.	OT Shield provides a hardware-enforced conduit consistent with recommended clinical/administrative segmentation.
CERT-In / Sectoral Health CERT Advisories	Maintain baseline security hygiene and incident reporting for healthcare infrastructure.	Reduces the clinical network attack surface that leads to reportable incidents; simplifies audit evidence.
Medical Device Cybersecurity Guidance	Deploy connected medical devices within segmented network architectures.	Provides a physically enforced segmentation layer for medical device networks without modifying the devices themselves.

Business Value

Business Driver	Impact of ChiefNET OT Shield
Patient safety	Removes the most common remote-attack vector into clinical device networks, reducing risk of ransomware-driven care disruption.
Regulatory & accreditation readiness	Provides a hardware-verifiable segregation control that is straightforward to demonstrate to auditors and accreditation bodies.
Operational cost	Eliminates recurring firewall patch cycles on networks connected to devices that are difficult or impossible to patch.
Digital health transformation pace	Allows EHR integration, analytics and remote monitoring initiatives to proceed without re-architecting clinical networks.
Multi-facility scalability	Centralised, zero-touch provisioning supports rollout across many hospitals and clinics from a single management platform.
Incident response	Rapid, low-risk access to device and facility logs speeds up investigation after a security or safety event.

ChiefNET OT Shield vs. Traditional Firewalls

In healthcare environments, where clinical devices often cannot be routinely patched and downtime can directly affect patient care, the distinction between rule-based and hardware-enforced isolation is a first-order design decision.

Dimension	ChiefNET OT Shield	Traditional Firewall
Data directionality	One-way, physically enforced	Two-way, governed by software rules

Dimension	ChiefNET OT Shield	Traditional Firewall
Patch / maintenance burden	None – isolation is hardware, not firmware	Frequent patching, difficult on regulated medical devices
Misconfiguration risk	Not applicable – no rule set to misconfigure	Common cause of real-world hospital ransomware incidents
Resistance to remote exploitation	Near-total – no reverse path exists to exploit	Moderate; depends on rule hygiene and patch currency
Fit for life-critical medical devices	Purpose-built for this class of asset	Adequate for hospital IT; not ideal for medical devices
Audit / compliance evidence	Physically demonstrable segregation	Requires ongoing rule and log review to evidence

Technical Capability Snapshot

Capability	Specification
Throughput	Up to 1 Gbps
Isolation	100% one-way, optical / hardware-enforced physical air gap
Software exploit surface on reverse path	Zero – no reverse channel exists
Protocols supported	BACnet, Modbus, MQTT, OPC UA, industrial UDP (broadcast/multicast/anycast)
Data / file transfer	UDP file transfer, Syslog, HTTP PUT
Transport security	Encrypted VPN tunnel from RX side to EHR/cloud endpoint
WAN connectivity (RX side)	Dual WAN with 4G/5G failover for uninterrupted delivery
Management	Cloud-hosted controller, zero-touch and pre-provisioning, fleet dashboards and alerting
Operating system	Hardened OS, minimised attack surface, no routine patch cycle required
Additional networking	Built-in SD-WAN for secure multi-facility interconnection alongside clinical network isolation

Deployment & Engagement Model

ChiefNET recommends a phased engagement for healthcare deployments, allowing providers to validate the solution at one representative facility or department before wider rollout.

Phase 1 – Assessment & Design

- Site survey of the target hospital or clinic: clinical network topology, connected medical devices, existing firewall/VPN posture.
- Identification of required data points (patient monitor feeds, imaging metadata, facility system logs) and target EHR/cloud destinations.
- Reference architecture finalised against HIPAA, ABDM and ISO 27799 segmentation expectations as applicable.

Phase 2 – Pilot Deployment

- OT Shield installed at one representative ward, department or facility, configured for the identified protocols and data flows.
- Validation of one-way data delivery, VPN transport and EHR/dashboard visibility with clinical and IT teams.
- Compliance walkthrough to confirm alignment with the provider's data protection policy and applicable regulations.

Phase 3 – Fleet Rollout (site-dependent)

- Zero-touch provisioning used to scale deployment across remaining departments, hospitals and clinics.
- Central health IT SOC dashboards extended to provide system-wide monitoring and alerting.
- Documentation and audit evidence packaged for regulatory and accreditation reviews.

Phase 4 – Ongoing Support

- ChiefNET provides device health monitoring, remote diagnostics support and periodic architecture reviews as the health system's data and analytics needs evolve.

Conclusion

Healthcare providers face a structural challenge: the same connectivity that enables modern patient care and digital health initiatives also expands the attack surface of clinical networks that directly affect patient safety. ChiefNET OT Shield resolves this tension directly – not by adding another rule set to manage, but by making the reverse path physically impossible.

Across hospitals, clinics and diagnostic centres, the use cases in this document show a consistent pattern: clinical data flows out for charting, analytics and reporting, while command-and-control risk is removed at the hardware level. For health systems balancing digital transformation against the non-negotiable safety requirements of patient care, that combination – visibility without exposure – is the foundation ChiefNET OT Shield is built to provide.

Next Step

ChiefNET recommends starting with a site assessment and pilot deployment at one representative ward, department or facility, validating data delivery and compliance alignment before scaling across the health system.

ChiefNET

About ChiefNET Private Limited

ChiefNET Private Limited, founded in 2020 and headquartered in Coimbatore, India, builds secure networking products for enterprises and critical infrastructure: ChiefNET SD-WAN, a cloud-managed network platform for multi-site organisations, and ChiefNET OT Shield, a hardware-enforced data diode for operational technology. ChiefNET product series are Make in India certified.

---

contact@chiefnet.io · chiefnet.io
DVP Building, First Floor, No. 4, Kalapatti Main Road, Civil Aerodrome Post, Nehru Nagar West, Coimbatore, Tamil Nadu 641014, India