ChiefNET

CHIEFNET SD-WAN · APPLICATION NOTE

Healthcare Multi-Campus Networking

Connecting hospital campuses, clinics and diagnostic labs to HIS, EHR and PACS

Healthcare · Diagnostics

Document reference	Version	Date	Published by
CN/SDW/AN/HEALTH/v1.0	1.0	November 2026	ChiefNET Private Limited

Contents

1. Overview
2. The Challenge
3. The ChiefNET Solution
4. Reference Architecture
5. Key Benefits
6. Capability Map
7. Deployment Summary
8. Conclusion

Also available online at chiefnet.io/use-cases/sd-wan/healthcare-multi-campus/

Overview

A modern healthcare provider rarely operates from a single building. A typical group runs one or two main hospital campuses, a ring of outpatient clinics, and diagnostic laboratories or imaging centres. Clinical work at every one of these locations depends on central systems: the Hospital Information System (HIS), Electronic Health Records (EHR), laboratory systems and the Picture Archiving and Communication System (PACS).

This application note shows how ChiefNET SD-WAN connects these locations to central applications in a data centre and in the cloud, with the encryption, availability and traffic control that clinical systems need.

The Challenge

Consider a healthcare group with two hospital campuses, 15 clinics and six diagnostic labs. HIS, EHR and PACS run in a private data centre, and the patient portal and an off-site image archive run in a public cloud VNET. The network team faces the following:

- **Clinical systems cannot wait.** Admissions, prescriptions, lab orders and results all flow through HIS and EHR. A slow or failed link at a clinic stops work at the front desk and in consultation rooms.
- **Imaging is bandwidth-heavy.** CT, MRI and X-ray studies are large. Moving them from labs to PACS, and from PACS to reading rooms at other campuses, can saturate a link and slow everything else.
- **Sensitive data on public links.** Patient records and images travel over Internet and broadband connections, so the traffic must be encrypted and kept away from untrusted paths.
- **Devices that should not reach the Internet.** Imaging modalities, lab analysers and other clinical devices often run older software and should communicate only with internal systems.
- **Mixed traffic.** Staff browsing, software updates and guest Wi-Fi share the same connections as clinical traffic.
- **Limited IT staff at remote sites.** Clinics and labs typically have no network specialist on site.

The ChiefNET Solution

ChiefNET deploys a pre-provisioned CPE at every location and joins them into a single private network through the ChiefNET Cloud WAN, managed from the ChiefNET Orchestrator.

Secure connectivity to central applications

Every CPE builds encrypted tunnels to the ChiefNET Cloud WAN using AES-256, with mutual X.509 certificate authentication for each device. Dynamic routing is preconfigured, so clinic and lab subnets are learned automatically and reach HIS, EHR and PACS without manual routing.

The data centre joins the network through a CN-VM-1 virtual CPE on VMware or KVM, and the cloud VNET through a CN-Cloud-1 instance. For the heaviest path, between the main campus and the data centre, ChiefNET's on-premises VPN server feature can create a direct site-to-site tunnel alongside the Cloud WAN, giving imaging traffic a short, dedicated route.

High availability at the main campus

A hospital campus cannot depend on a single device. ChiefNET Edge Device HA deploys two CN-4 appliances as a VRRP hot-standby pair. Each device monitors the other; if an interface or the whole active device fails, for example because of a local power fault, the standby takes over the gateway role.

Each CPE can also use two WAN links. ChiefNET continuously measures packet loss, latency and jitter on each link and on each tunnel, and moves traffic to the better path when configured thresholds are crossed. Each CPE also operates autonomously and does not need continuous contact with the Orchestrator to keep the site running. A full backup of each device configuration is held centrally, so a replacement unit can be configured identically to the one it replaces.

Quality of service for clinical and imaging traffic

ChiefNET's QoS engine, built on hierarchical fair-share scheduling, lets administrators classify traffic by subnet, port, protocol or application domain and apply a profile:

- **Minimum bandwidth** for HIS and EHR traffic, so that clinical transactions remain responsive at all times.
- **Minimum and maximum bandwidth** for PACS transfers, so that studies move quickly without taking the whole link.
- **Real-time** profiles for VoIP and IP PBX traffic between campuses.
- **Maximum bandwidth** limits for non-clinical traffic such as updates and streaming.

With a CN-4 supporting up to 800 Mbps of VPN throughput, a campus or imaging centre has capacity for large study transfers alongside everyday traffic.

Keeping clinical devices and data private

Imaging modalities, lab analysers and similar devices can be configured as **enterprise-only systems**: they communicate with PACS, LIS and HIS over the tunnels but cannot reach the Internet directly. With **sensitive-traffic exclusive forwarding**, selected clinical traffic can be restricted to specific trusted WAN or tunnel paths; if that path is unavailable, the traffic is held back rather than sent over an untrusted link.

Split-horizon DNS sends lookups for internal host names to the organisation's own DNS servers, so that internal names are never exposed to ISP resolvers. VLAN interfaces and traffic policies separate clinical networks from guest Wi-Fi, and guest traffic can be limited to local Internet breakout only.

Network-level protection at every site

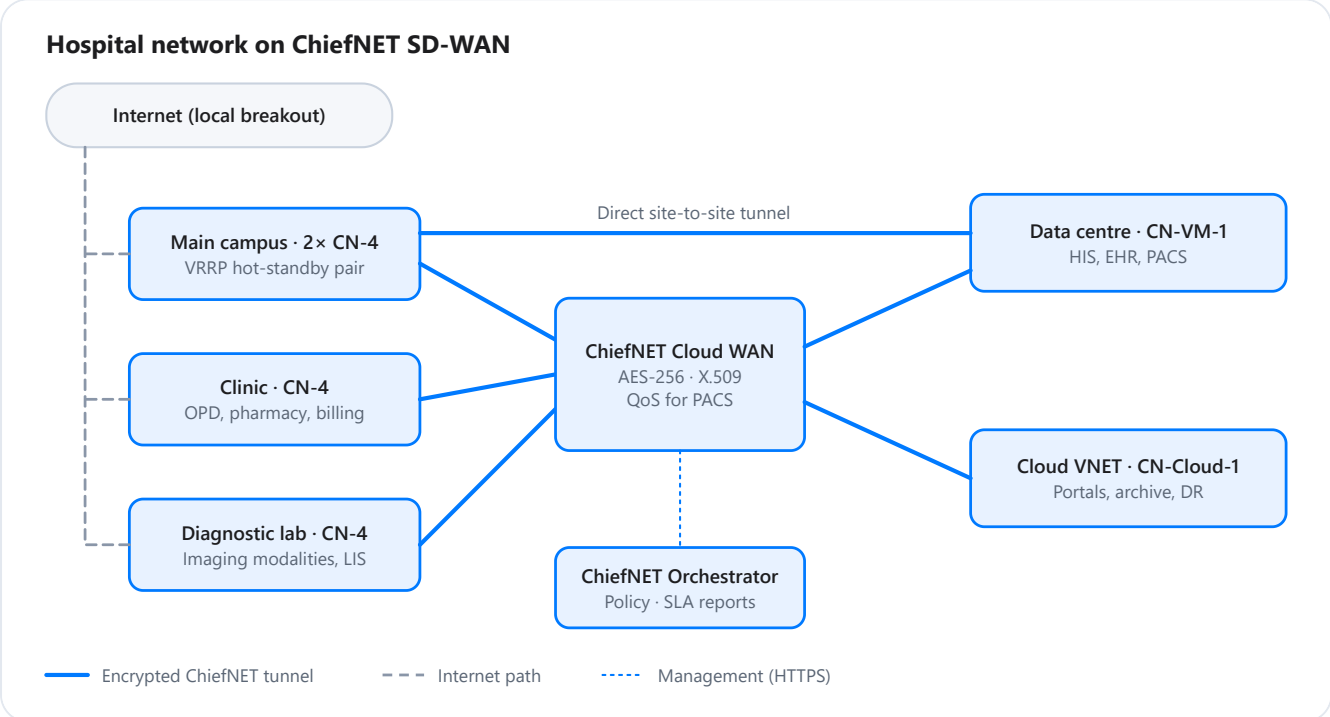
Every CPE has no open WAN ports and initiates all connections itself. DNS filtering with curated blocklists blocks malware, phishing and other unwanted domain categories across all sites, and application control can drop or limit unwanted applications. Where content-level inspection is also required, ChiefNET can be integrated with Palo Alto Networks Prisma Access on a per-site basis.

Controlled administration

Orchestrator access uses two-factor authentication, with full administrator and read-only administrator roles. Every configuration change and every new device provisioning raises an event, and the event log can be exported as CSV for internal audit.

Reference Architecture

The diagram shows the main campus with a redundant pair of CN-4 CPEs, a clinic and a diagnostic lab connected through the ChiefNET Cloud WAN to a data centre (CN-VM-1) hosting HIS, EHR and PACS, and to a cloud VNET (CN-Cloud-1) hosting portals, archive and disaster recovery. A direct tunnel links the main campus and the data centre. Non-clinical Internet traffic breaks out locally at each site.



Campuses, clinics and labs reach HIS, EHR and PACS in the data centre and cloud over ChiefNET Cloud WAN, with a direct tunnel and redundant CPEs at the main campus.

Key Benefits

- **Dependable clinical access.** Redundant CPEs, dual links and autonomous operation keep HIS and EHR reachable during equipment or ISP failures.

- **Faster imaging workflows.** Bandwidth guarantees and a direct campus-to-data-centre tunnel move large studies without disrupting other work.
- **Patient data stays private.** AES-256 encryption, exclusive forwarding and split-horizon DNS keep records and internal names off untrusted paths.
- **Clinical devices are contained.** Enterprise-only policies stop modalities and analysers from reaching the Internet.
- **Low on-site effort.** Clinics and labs receive pre-provisioned CPEs that need only power and cables.
- **Clear accountability.** Role-based access, two-factor login and exportable change logs support internal governance.

Capability Map

ChiefNET capability	How it is used here
ChiefNET Cloud WAN with dynamic routing	Connects campuses, clinics and labs to the data centre and cloud VNET
On-premises VPN server (direct tunnel)	Provides a dedicated path between the main campus and the data centre for PACS
Edge Device HA (VRRP hot-standby)	Keeps the main campus gateway available if a CPE or interface fails
Link-quality monitoring and failover	Moves clinical traffic to the better WAN link on loss, latency or jitter
Hierarchical QoS	Guarantees bandwidth to HIS and EHR, and bounds PACS transfers
Enterprise-only systems and exclusive forwarding	Keeps modalities and sensitive traffic on trusted enterprise paths
Split-horizon DNS and DNS filtering	Protects internal names and blocks malicious domains
CN-VM-1 and CN-Cloud-1	Brings the private data centre and cloud VNET into the same network

Deployment Summary

1. Map campuses, clinics and labs, and list central applications with their servers, ports and expected traffic volumes.
2. Plan an HA pair for each main campus and dual WAN links where available.
3. Deploy CN-VM-1 in the data centre and CN-Cloud-1 in the cloud VNET; configure the direct campus-to-data-centre tunnel.

4. Define QoS, enterprise-only and DNS policies in the ChiefNET Orchestrator, then ship pre-provisioned CPEs to each site.
5. Verify failover, HIS/EHR response times and PACS transfer rates, and enable alerts and SLA reports.

Conclusion

Healthcare delivery spread across campuses, clinics and labs needs a network that is private, resilient and predictable. ChiefNET SD-WAN connects every location to HIS, EHR and PACS through encrypted tunnels, protects clinical traffic with bandwidth guarantees and redundant gateways, and keeps clinical devices away from the Internet. Central management lets a small IT team run the whole network without visiting every site.

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.

---

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