

The Cloud Prescription

Why MedTech Needs a Stronger Digital Backbone



The Fault in Our Networks

The promise of modern medicine hinges on speed—the speed of diagnosis, treatment, and data. But when networks falter, that speed vanishes, replaced by delays, errors, and uncertainty. In a world where seconds can mean the difference between life and loss, healthcare's greatest weakness isn't a lack of innovation but reliable connectivity. Imagine the following nightmares:

- **A radiologist in Bengaluru** loads a 3D scan of a patient's brain tumour, only to find that the image resolution has degraded due to unstable bandwidth.
- **A telemedicine session** in a tier-2 hospital stalls mid-consultation as the connection drops.
- **A cloud-based AI diagnostic tool** designed to detect early-stage cancer sits idle, waiting for data to sync from multiple facilities.

India's MedTech revolution is being held hostage by bad networking.

While the industry has leapt forward in AI-powered diagnostics, telehealth, and connected medical devices, the digital infrastructure supporting it remains riddled with bottlenecks. The disconnect between MedTech innovation and network capability directly threatens patient care, operational efficiency, and revenue streams.

The numbers tell a sobering story. A 2023 Frost & Sullivan report found that 42% of healthcare IT leaders in India cite unreliable network connectivity as their biggest operational challenge. More than 65% of diagnostic centers struggle with bandwidth issues when transferring large imaging files, affecting their ability to process results on time.

MedTech firms, hospitals, and diagnostic labs now find themselves at a crossroads. They can either endure network outages and slowdowns, accepting inefficiencies as the cost of business, or they can upgrade to cloud-managed networking solutions that ensure uninterrupted connectivity, security, and scalability.

For those choosing the latter, cloud-managed networking solutions like Cisco Meraki SD-WAN are quietly reshaping the digital backbone of healthcare, ensuring reliability, security, and scale where it matters most. Let's discover how.

Beyond Wires and Cables: The MedTech Cloud Imperative

A decade ago, hospitals relied on localised servers, on-premise data storage, and legacy networking hardware. Today, AI-powered radiology tools, robotic surgery systems, and real-time patient monitoring devices generate petabytes of data that must be transmitted, processed, and preserved in the cloud.

Still, a large number of MedTech firms and healthcare providers rely on outdated MPLS connections. MPLS (Multiprotocol Label Switching) connections are a legacy networking technology used by many hospitals, diagnostic labs, and healthcare IT systems to ensure private, high-priority data transmission between locations. Unlike traditional routing, MPLS creates dedicated, pre-defined paths for data, allowing for more predictable performance compared to standard broadband connections.



While MPLS was once the gold standard for secure and stable networking, its limitations are becoming increasingly evident in modern AI-driven, cloud-first healthcare environments.

Why MPLS Struggles in Healthcare IT

- **High Latency for AI & Imaging**

Medical imaging transfers (MRI, CT scans, PACS systems) generate terabytes of data every single day. MPLS struggles with high-latency routing, delaying diagnostics.

AI-powered healthcare tools require real-time access to cloud computing resources, but MPLS does not dynamically optimise traffic, leading to bottlenecks during peak loads.

- **Expensive & Difficult to Scale**

Expanding telemedicine services, diagnostic labs, and multi-location hospital chains requires rapid network deployment.

MPLS circuits take weeks to months to provision in new locations, significantly delaying expansion efforts.

Bandwidth upgrades are costly, requiring hardware overhauls instead of simple cloud-based adjustments.

- Limited Cloud Compatibility

Cloud-hosted EHRs (Electronic Health Records), AI-driven patient monitoring, and remote healthcare solutions demand agile, software-defined networks.

MPLS was not designed for cloud-native applications, resulting in poor performance when routing traffic between cloud providers and on-premises hospital infrastructure.

- Lack of Built-in Security & Compliance

Ransomware attacks on hospitals increased by 94% in the past year (IBM Security Report, 2024), yet MPLS lacks integrated Zero Trust security, automated threat detection, or real-time encryption enforcement.

Cisco Meraki SD-WAN, in contrast, embeds security directly into the network, protecting healthcare data at every touchpoint.

The Shift from MPLS to SD-WAN in Healthcare

Hospitals and MedTech firms adopting AI, remote patient monitoring, and telemedicine networks need faster, scalable, and cloud-optimised networking solutions. Cisco Meraki SD-WAN intelligently routes traffic, secures patient data, and enables near-zero downtime—without the limitations of traditional MPLS. SD-WAN allow MedTech firms to:

- Ensure seamless data flow across geographically distributed facilities
- Enable AI-powered diagnostics with real-time data streaming
- Reduce IT complexity with centralized, automated management
- Minimise downtime with built-in failover mechanisms



MPLS vs SD-WAN Cost-Benefit Comparison

	Feature	MPLS	Cisco Meraki SD-WAN
1.	Latency & Performance	Higher latency, struggles with large AI & imaging workloads	Optimized for AI, imaging, and real-time healthcare data
2.	Scalability	Difficult to scale, requires lengthy provisioning times	Scalable within hours, cloud-based configuration
3.	Cloud Compatibility	Not optimized for cloud applications, requires manual routing	Native cloud integration with AWS, Azure, and Google Cloud
4.	Security	No built-in Zero Trust security, requires separate firewall solutions	Built-in security with Zero Trust access, encrypted tunnels
5.	Cost & Deployment Time	Expensive, bandwidth upgrades require major infrastructure changes	Lower TCO, fast deployment with centralized management
6.	Redundancy & Failover	Limited redundancy, high risk of downtime during outages	Automated failover, ensures near-zero downtime

Hospitals and Clinics Are Drowning in Data. AI is Making the Flood Worse

For years, hospitals relied on human experience-based decision-making. Today, AI-driven diagnostics are transforming how doctors detect diseases, optimise treatments, and personalise patient care. But there's a problem—AI models are only as good as the data they receive, and networks are struggling to keep up.

AI in Diagnostics: More Data, More Complexity, More Downtime Risks

India is at the forefront of AI adoption in healthcare, with MedTech startups and research labs deploying deep learning models for faster, more accurate diagnoses. But these AI applications generate massive workloads that demand high-speed, uninterrupted network connectivity.

Consider a typical AI-powered pathology lab:

- A hospital in Mumbai sends tissue biopsy scans to an AI algorithm hosted in a cloud data center in Bengaluru. The AI detects cancerous cell patterns with an **accuracy rate of 94%, improving** upon human pathologists who typically **average 85-90% accuracy**. *(Source: The Lancet, 2023).*
- The AI needs to process gigabytes of high-resolution histopathology images in real-time and send the results back.
- If the network lags, doctors are left waiting—a delay that could cost a patient precious treatment time.

This is not an isolated case. AI models used in radiology, genomics, and ICU patient monitoring require:

- **Ultra-low latency (< 50ms)** to transfer large datasets for real-time decision-making.
 - **Uninterrupted cloud connectivity** for AI-powered second opinions and predictive diagnostics.
 - **High network security** to prevent tampering with AI training data, which cybercriminals are increasingly targeting.
-

Yet, more than 60% of Indian hospitals and MedTech firms run AI workloads over legacy MPLS networks, which were never built for this kind of demand.

(Source: NASSCOM Healthcare IT Report, 2024).

Why AI and Cloud Networking Must Go Hand-in-Hand

AI-driven MedTech solutions do not function in isolation. They require a continuous loop of data processing, transmission, and real-time updates, meaning network failures are not just a minor inconvenience—they are a direct threat to AI-driven healthcare outcomes.

Here's why cloud-managed SD-WAN is the only practical solution for AI-powered MedTech applications:

1. Real-Time Image Processing: When Every Second Counts

Medical imaging AI models, used for early stroke detection and cancer screening, need to analyse terabytes of CT scans, MRIs, and X-rays. Any delay in processing means delayed diagnosis, which directly impacts patient outcomes.

- With Cisco Meraki SD-WAN, AI models receive continuous, uninterrupted access to cloud-hosted medical imaging datasets.
- Smart traffic routing prioritises medical data over non-essential hospital applications, ensuring zero lag in image transmission.
- Redundant network failovers prevent AI workloads from stalling during network disruptions.

Example:

*A cloud-based AI tool analysing heart attack risks can identify **early warning signs up to 6 hours before symptoms appear**, but only if real-time ECG data is available without network bottlenecks.*

2. Training the AI Brain: Data Bottlenecks Slow Down Learning

AI models learn by ingesting vast amounts of patient data, but training them requires uninterrupted access to high-speed cloud computing infrastructure.

- Traditional networks limit bandwidth availability, slowing AI training cycles.
- Meraki's AI-powered bandwidth optimisation ensures that machine learning (ML) workloads receive the network priority they need without being disrupted by administrative tasks like email syncs and software updates.

Example:

A genomics research facility using AI for DNA sequencing requires transferring oceans of data between labs. If the network can't handle the load, AI predictions take days instead of hours, delaying breakthroughs in disease treatments.

3. Cybersecurity for AI: The Data Shield MedTech Needs

AI models in healthcare work with highly sensitive patient data, making them a prime target for cybercriminals. A 2023 IBM report found that healthcare AI systems are 3x more likely to be attacked than AI in other industries because:

- AI models can be poisoned by tampering with training data.
- Ransomware can lock hospitals out of AI-powered diagnosis tools

Cisco Meraki SD-WAN combats these threats by integrating:

- Zero Trust Network Access (ZTNA) – Ensuring only authorised personnel can access AI-powered systems.
- End-to-End Encryption – Preventing unauthorised interception of AI training datasets.
- AI-Powered Intrusion Detection – Identifying anomalies that signal a potential cyberattack before it happens.

Example:

An AI model used for predicting patient deterioration in ICUs can be rendered useless if its data sources are compromised. Cloud-managed networking ensures AI remains secure and functional.

AI-Powered Healthcare Needs AI-Optimised Networks

AI is not the future of MedTech—it's the present. Indian healthcare firms investing in AI-driven diagnostics, personalised medicine, and remote patient monitoring must recognise a fundamental truth:

Without a strong networking foundation, AI in healthcare will always fall short of its potential.

The solution is clear: AI-powered healthcare needs AI-optimised networking. Cisco Meraki SD-WAN provides:

- High-speed, low-latency network infrastructure built for AI workloads.
- Real-time traffic prioritisation, ensuring AI gets the bandwidth it needs.
- Cloud-native scalability, allowing hospitals to expand AI models without bottlenecks.
- Automated security layers to protect AI-driven MedTech applications.

Proactive Data Systems is helping Indian MedTech firms and hospitals bridge the AI-networking gap.

Why Cisco Meraki is the Answer to MedTech's Connectivity Woes

Cisco Meraki SD-WAN isn't just faster internet—it's an intelligent networking framework designed for mission-critical healthcare environments.

1. 99.99% Uptime: No More "Network Down" Excuses

- Automated failover to secondary links keeps MedTech services online.
- Intelligent traffic steering prioritizes life-critical applications over routine admin work.

2. Zero Trust Security: Because a Breach in MedTech is a Breach of Life

- End-to-end encryption for patient data prevents cyber threats.
- Zero Trust Network Access (ZTNA) ensures only authorized users access systems.

3. One Dashboard, Total Control: IT Simplified

- Manage thousands of distributed healthcare facilities from a single cloud dashboard.
- AI-powered anomaly detection identifies network issues before they cause failures.

4. Instant Scalability: Open a New Clinic in Weeks, Not Months

- No need for complex MPLS configurations—deploy new locations with zero-touch provisioning.
- Cloud-managed firewalls ensure compliance with HIPAA, GDPR, and India's Digital Personal Data Protection Act (DPDPA).

Hospitals and MedTech firms no longer need massive IT teams to maintain their networks—Meraki's AI-driven automation does the work.

The Future of MedTech Networks: A Cloud-First Strategy

Healthcare is no longer just about doctors and patients. It's about data, algorithms, real-time insights, and connected devices. The backbone of modern medicine isn't just innovation—it's reliable, high-speed, and secure connectivity.

For MedTech firms and healthcare IT leaders, the question is no longer whether to upgrade their networking, but how soon.

Proactive Data Systems, in partnership with Cisco, is helping leading hospitals, diagnostics chains, and MedTech startups move to cloud-managed networking with zero downtime, ironclad security, and effortless scalability.

Let's build the digital backbone for MedTech together. Get in touch today to explore Cisco Meraki's role in your healthcare IT strategy.

Write to us at pro@proactive.co.in to book an expert consultation.
