PROACTIVE™
Enhancing Digital Experience

Clinical-Grade Wi-Fi for Indian Hospitals: A Design Guide for CIOs and Biomed Leads.

MRI rooms, radiology bays, ICU floors, bedside coverage, medical-device segmentation, and NABH-ready evidence. From site survey to steady state.

Version 1.1 · Updated August 2026 ·

Reflects DoT 6 GHz delicensing (January 2026), IEC 80001-1:2021 medical-device network risk management, NABH 6th Edition Accreditation Standards for Hospitals (mandatory from 1 January 2025), and DPDP Rules (notified 13 November 2025).

Proactive Data Systems Healthcare Practice

Cisco Preferred Partner across Networking, Security, Collaboration, Data Center, and Services · Cisco Advanced Customer Experience Specialised · Since 1991.

Preface

Hospital Wi-Fi is different from office Wi-Fi in ways that only reveal themselves after the first go-live. Faraday-cage-shielded MRI rooms swallow every RF signal that reaches them. ICU beds are separated by fabric curtains that reflect and absorb 2.4 GHz signal differently from 5 GHz. Medical infusion pumps expect uninterrupted association with a nursing-station gateway that runs on a Windows OS nobody has patched since 2016. Radiologist workstations pull hundreds of megabytes of image data per scan retrieval, and expect the network to move that data in seconds.

This field guide is written for the hospital CIO, biomed engineering lead, or IT infrastructure head who has done at least one Wi-Fi refresh, knows what went wrong last time, and wants a working reference for how to do the next one properly. It covers site survey discipline, ceiling design, spectrum choices, medical-device segmentation aligned to IEC 80001-1:2021, and the evidence NABH assessors ask for under the current 6th Edition standards.

It is written by the Proactive Data Systems Healthcare Practice, from live implementations at tertiary care hospitals, speciality medical groups, and diagnostic networks across India. It is deliberately opinionated on ceiling design, current on India's 6 GHz spectrum status following DoT's January 2026 delicensing, and free of vendor sales language beyond what is technically load-bearing. Consult your biomed engineering lead, your radiology head, and your compliance function before acting on any specific design decision.

In Brief

What Proactive Delivers for Hospital Wi-Fi:

Predictive site survey using Ekahau AI Pro or iBwave Wi-Fi. Clinical-grade coverage design for MRI rooms, radiology bays, ICU floors, wards, outpatient, and hostels. IEC 80001-1:2021-aligned medical-device network segmentation using Cisco Cyber Vision for device discovery and behavioural anomaly detection. Wi-Fi 6, Wi-Fi 6E, or Wi-Fi 7 access point selection matched to clinical space and India-market SKU availability.

Integration with HIS platforms (Epic, Oracle Health (formerly Cerner), athenahealth (formerly GE Centricity), Veradigm (formerly Allscripts), and Indian HIS platforms including Bahmni, Suvarna, Insta HMS, Medixcel, Napier HIS, and HealthPlix). NABH 6th Edition IMS chapter-mapped evidence packs. The Proactive Clinical-Grade Wi-Fi Design Guide for Indian Hospitals is available as a free download.

Who this is for:

CIOs, CTOs, Heads of IT, and biomed engineering leads at hospital chains, standalone tertiary care hospitals, speciality medical groups, diagnostic networks, and academic medical centres operating in India.

Since:

1991. Proactive Data Systems is a Cisco Preferred Partner across five portfolios and Cisco Advanced Customer Experience Specialised.

What Does "Clinical-Grade Wi-Fi" Actually Mean in an Indian Hospital?

Clinical-grade Wi-Fi is Wi-Fi that meets four operating standards simultaneously: it reaches every space where clinical work happens, including RF-shielded rooms and bedside positions; it stays associated with medical devices that cannot roam mid-session; it segments those medical devices from admin and guest traffic per IEC 80001-1:2021, and it produces the audit evidence NABH assessors and biomed engineering leads need to sign off on the estate.

Office-grade Wi-Fi meets none of these. It is designed for a workforce of laptops and phones held by adults who can walk to a better signal. It is not designed for a network-attached infusion pump on a bed that cannot move, or a portable ultrasound wheeled between wards, or a bedside patient monitor that has to hand off cleanly when the patient is transferred to the ICU.

The four operating standards translate into four working design principles:

- **Ubiquitous Coverage.**
  Every bed, every radiologist station, every nursing station, every MRI console, every OT (operating theatre) — each one has planned Wi-Fi coverage with predictive site survey backing.

- **Session Persistence For Medical Devices.**
  Devices that maintain long-lived TCP sessions (patient monitors, infusion pumps, ventilator telemetry) get network conditions that don't drop association. This drives 5 GHz preference, controlled roaming, and often a dedicated SSID with strict authentication.

- **IEC 80001-1:2021 Segmentation.**
  Medical devices sit in a network zone with only the specific communication paths their clinical function requires. Cross-zone communication to HIS and PACS runs through inspected paths.

- **Auditable Evidence.**
  Every SSID, every VLAN, every access rule, every device inventory, every configuration change is captured in a format the NABH assessor and the biomed engineering lead can review together.

What Wi-Fi Standards and Frequencies are Deployable in Indian Hospitals Today?

Indian hospitals in late 2025 and 2026 have three practical Wi-Fi generation choices: Wi-Fi 6 (802.11ax) for cost-optimised refreshes and the deployed base most refreshes are moving from, Wi-Fi 6E (802.11ax with 6 GHz support) for current builds now that DoT has delicensed the lower 6 GHz band, and Wi-Fi 7 (802.11be) for future-forward deployments where the ceiling design and client ecosystem justify the investment.

The spectrum picture in India as of 2026 is: 2.4 GHz (802.11b/g/n/ax) unlicensed and universally deployed but crowded; 5 GHz (802.11a/n/ac/ax) delicensed with substantial channel availability and appropriate for most enterprise use; and 6 GHz (5925–6425 MHz), delicensed by DoT in January 2026 through the "Use of Low Power and Very Low Power Wireless Access System including RLAN in Lower 6 GHz Band (Exemption from Licensing Requirement) Rules, 2026." Indoor and low-power outdoor Wi-Fi in the delicensed 6 GHz band is now permitted, unlocking Wi-Fi 6E and Wi-Fi 7 6 GHz operation for Indian hospitals.

The comparison table below summarises the practical hospital deployment view.

Wi-Fi Generation	IEEE Standard	Spectrum	Best Hospital Use Case	Cisco AP Options	Meraki AP Options	India Availability
Wi-Fi 6	802.11ax	2.4 GHz, 5 GHz	Cost-optimised refreshes; general wards; admin areas	Catalyst 9105, 9115, 9120	MR46, MR44 (EoS 31 Dec 2026 for MR46)	Available
Wi-Fi 6E	802.11ax (6 GHz extension)	2.4 GHz, 5 GHz, 6 GHz	High-density outpatient, radiology reading rooms, ICU floors	Catalyst 9162, 9164, 9166	MR57	Available (6 GHz delicensed Jan 2026)
Wi-Fi 7	802.11be	2.4 GHz, 5 GHz, 6 GHz (with wider channels and MLO)	Future-forward flagship deployments; PACS-adjacent reading rooms; forward-looking hospital chains	Catalyst 9172, 9176, 9178, 9179	Wi-Fi 7 Meraki series (verify current India SKU)	Emerging (client ecosystem maturing)

For most Indian tertiary care hospitals doing a refresh in 2025 or 2026, the practical recommendation is Wi-Fi 6E on Cisco Catalyst 9166I (indoor, wall or ceiling mount, five-radio design supporting 2.4 GHz and 5 GHz and 6 GHz simultaneously plus a dedicated 2.4 GHz IoT radio and BLE) or Cisco Meraki MR57 depending on management preference. Wi-Fi 7 access points from the Catalyst 9172/9176/9178/9179 series can be specified where the ceiling design and cabling investment justify future-proofing.

Frequency selection per clinical space follows a physics-first logic:

2.4 GHz- Best penetration through obstacles, but crowded and slow. Reserve for legacy medical devices that require it, or for coverage in areas where 5 GHz cannot penetrate.

5 GHz- The workhorse. Better throughput, cleaner channels, adequate penetration through most hospital walls. Default for staff, patient BYOD, and modern medical devices.

6 GHz- Cleanest spectrum, widest channels, best for high-density areas (nursing stations, radiologist reading rooms, OT scheduling stations). Requires Wi-Fi 6E or Wi-Fi 7 client devices to use.

For medical devices, spectrum choice is driven by what the device supports. Legacy telemetry systems and infusion pumps often only support 2.4 GHz. Modern patient monitors from GE HealthCare, Philips Healthcare, Mindray, and BPL Medical support 5 GHz. Design should accommodate both, with dedicated SSIDs per class of device where required.

How Do You Design Wi-Fi for MRI Rooms and Radiology Bays?

MRI rooms are purpose-built Faraday cages engineered to prevent external RF from contaminating the scanner's Larmor signal (approximately 64 MHz at 1.5T, 128 MHz at 3T) and to contain the scanner's own RF pulses. Wi-Fi signal from outside the room does not enter. Wi-Fi signal from inside the room does not leave. Every access point that serves an MRI room must be located inside the shielded envelope with a purpose-designed cable pathway through the RF-sealed penetration point.

The design approach that works is a single access point mounted at the operator console side of the MRI room (never on the magnet-facing wall), fed by a dedicated Cat 6A or fibre run through the room's RF-sealed cable penetration, with the access point's antennas pointed away from the magnet bore. Cisco Catalyst 9166I or Meraki MR57 access points with enclosure-mounted antennas at the shielded boundary is a common working design.
For radiology reading rooms - where radiologists pull large image files from PACS - high-density access point placement with 5 GHz or 6 GHz preference is the standard design. Reading rooms typically house four to twelve radiologist workstations in a compact footprint; a single ceiling-mount access point per room with 6 GHz support handles the density and the PACS-retrieval throughput.

For radiology bays outside the MRI suite (CT rooms, X-ray, ultrasound, fluoroscopy), the design is closer to standard hospital Wi-Fi with attention to the specific radiation-shielding materials in the room walls. Lead-lined walls in CT and X-ray rooms attenuate signal significantly; a ceiling-mount access point inside each shielded room is typically required, not shared coverage from the corridor.

The critical operational detail: for any MRI, CT, or radiology console, the clinician's Wi-Fi phone or tablet is not a substitute for the wired clinical console. Wired handsets on the imaging console for clinical communication that must not depend on RF is the design principle. Wi-Fi is for the radiologist's laptop, the technician's tablet, and the guest device - not for the imaging modality itself.

How Do You Cover Bedside and ICU Wi-Fi Reliably?

Bedside and ICU Wi-Fi coverage is achieved through predictive site survey using Ekahau AI Pro or iBwave Wi-Fi, with drawn-curtain and open-curtain RF modelling, and a ceiling access point every three to four ICU beds. Access point spacing is tighter than a general ward because medical device density is higher and session persistence for patient monitors, infusion pumps, and ventilators matters more.

The typical ICU has 8 to 20 beds separated by fabric curtains that behave differently from walls in RF terms. Patient monitors, ventilators, infusion pumps, and dialysis machines cluster at each bed. Nursing stations sit at the centre or the corridor edge. Coverage that looks fine on a heatmap can fail at specific bed positions when the curtains are drawn.

The design pattern that works: a ceiling-mount access point every three to four ICU beds, with predictive site survey accounting for curtain positions in both drawn and open states.
For general wards (multi-bed rooms with fewer connected medical devices), ceiling access point spacing of every six to eight beds is typically adequate. For private rooms and daycare bays, a single ceiling access point per two-to-three rooms handles typical density.

For bedside patient BYOD (patients on Wi-Fi calls with family, streaming, browsing), a distinct guest SSID with bandwidth caps prevents patient traffic from degrading clinical traffic. The guest SSID lives on a segmented VLAN that cannot reach any clinical or admin network.

Roaming behaviour matters. Medical devices on the clinical SSID should roam smoothly between access points as patients are wheeled from ICU to OT to recovery. This requires consistent SSID broadcast, aligned RSSI thresholds, and 802.11k/v/r fast-roaming (Radio Resource Measurement, BSS Transition Management, and Fast BSS Transition respectively) enabled and tested with the specific medical device families in use. Some legacy medical devices do not support 802.11r - verify per device before enabling.

Nurse call systems - Ascom Telligence, Rauland Responder 5, Baxter (Hillrom) NaviCare, Stryker Vocera Smartbadge, or Cisco Webex Wireless Phone - often overlay on the Wi-Fi. If they do, the Wi-Fi coverage design must include the nurse call platform's specific coverage and hand-off requirements, tested against the vendor's design guide.

How Do You Segment Medical Devices From Admin Networks per IEC 80001-1:2021?

IEC 80001-1:2021 requires hospitals to treat the network as part of the medical device ecosystem, with formal risk management aligned to ISO 31000 across three properties: safety, effectiveness, and security.

In practice, this means medical devices sit in a network zone (typically a dedicated VLAN or set of VLANs) with only the specific network paths their clinical function requires, and cross-zone communication to HIS, PACS, LIS, and nurse call platforms runs through pre-approved paths inspected at a next-generation firewall.

IEC 80001-1:2021 supersedes the 2010 edition and reframes the standard around the three-property risk model, aligned to ISO 31000. The 2021 revision also strengthens the documented responsibility agreement between IT, biomed engineering, and clinical operations, and adds change control expectations for network changes that affect medical devices.

The operational translation is straightforward. Communication with the HIS, PACS, LIS, and nurse call platform runs through pre-approved paths inspected at a next-generation firewall (Cisco Secure Firewall, Palo Alto NGFW, or Check Point). Communication from the biomed zone to the admin network, the internet, or any other unrelated zone is denied by default.

Cisco Cyber Vision (part of Cisco's Industrial Threat Defence architecture, integrated with Cisco Identity Services Engine and Cisco Secure Firewall) is the discovery and monitoring layer that makes this manageable at scale. It passively identifies every medical device on the network, classifies it by function (imaging, monitoring, infusion, dialysis, laboratory), and monitors for behavioural anomalies. New devices attaching to the network are flagged for biomed engineering review before they receive full network access.

The zoning pattern that works in practice:

Zone 1: Life-Support and Tier-0 Devices (ventilators, dialysis machines, cardiac monitoring in ICU). Strictest segmentation, no internet reachability, communication only with authorised nursing station and HIS integration.

Zone 2: Imaging and Diagnostic Devices (CT, MRI, X-ray, ultrasound). Segmented from admin network; communication with PACS through inspected path.

Zone 3: General Clinical Devices (infusion pumps, patient monitors, vital signs stations). Segmented from admin; communication with HIS and nurse call through inspected paths.

Zone 4: Biomed Engineering Management Network. Only biomed engineering staff can reach this zone; no clinical traffic. Used for device firmware updates, configuration changes, and health monitoring.

Zone 5: Admin, Clinical Staff, and BYOD. Standard corporate segmentation; no route to biomed zones except through the inspected paths.

Zone 6: Guest and Patient BYOD. Fully isolated; only internet reachability.

The IEC 80001-1:2021 risk file for the network includes: device inventory by zone, communication path documentation, change control records, incident response evidence, and periodic risk reviews signed off jointly by the IT lead, the biomed engineering lead, and the clinical operations lead.

How Do You Handle High-Density Wards, Outpatient Clinics, and Waiting Areas?

High-density outpatient and waiting-area Wi-Fi is designed for peak concurrent client counts of 400 to 800 per clinic, with ceiling access points every 6 to 8 metres in waiting areas and tighter every 4 to 5 metres in consultation rooms. Guest SSID authentication is via captive portal integrated with HIS registration or phone-verified OTP, with per-client bandwidth caps of 2 to 5 Mbps to prevent one streaming session from degrading clinic operations.

A typical outpatient wing sees 100 to 400 patients at peak, each carrying two to three devices. Combined with clinic staff devices, the concurrent client count per clinic can exceed 800.

Cisco Catalyst 9166I or Meraki MR57 access points handle the client density; client-load balancing enabled at the controller level prevents single access point saturation.
Consultation rooms need separate Wi-Fi treatment. Doctors' laptops, tablets, and dictation devices connect to the corporate clinical SSID. Consultation-room design often includes wall-mount or under-desk access points for consistent signal despite the small enclosed space.

Waiting-area digital signage, self-service kiosks, and check-in tablets connect on a dedicated SSID with static provisioning. Not on the corporate SSID, not on the guest SSID, a distinct management SSID that keeps device inventory clean.

Registration desks and billing counters use ruggedised handsets and wired workstations where possible; Wi-Fi is available but not the primary path for transaction-critical activity.

How Does Wi-Fi Interact With PACS and HIS?

Wi-Fi is the access layer; PACS and HIS are the transactional and image-retrieval spine. Wi-Fi has to deliver 200 to 500 Mbps sustained throughput per client for PACS scan retrieval in radiologist reading rooms, and under 50 ms round-trip latency to the HIS backend for a responsive user experience. These are the specific numbers that decide whether the Wi-Fi is clinically usable, not just technically live.

PACS (Picture Archiving and Communication System) demands high-throughput retrieval for CT and MRI scan viewing. A single CT scan is 100 to 500 MB; an MRI scan can be several gigabytes. Radiologist workstations pulling scans over Wi-Fi need consistent 200 to 500 Mbps sustained throughput per client for a responsive experience. Reading rooms should have 6 GHz Wi-Fi (now available with DoT's January 2026 delicensing), wired backhaul from the access point to the switch at 2.5 Gbps or higher, and the access point uplink switch connected to the PACS storage tier through a low-hop network path.

HIS (Hospital Information System): Epic, Oracle Health (formerly Cerner), athenahealth (formerly GE Centricity), Veradigm (formerly Allscripts), or Indian HIS platforms (Bahmni, Suvarna HIS, Insta HMS, Medixcel, Napier HIS, HealthPlix) - is transactional. Individual HIS queries are small (typically under 1 MB) but need consistent low latency. Wi-Fi to HIS backend latency should stay under 50 ms round-trip for a responsive user experience.

Bed-side Patient Monitors: (Philips IntelliVue, GE HealthCare CARESCAPE, Mindray BeneVision) integrate with the HIS through the biomed zone. Wi-Fi association must be persistent; roaming during a patient transfer from ICU to OT should be seamless. Test with actual patient monitors on the deployed Wi-Fi before go-live, not just with laptops.

How Does Wi-Fi Interact With Nurse Call Systems?

Nurse call systems on Wi-Fi require strict quality-of-service treatment because nurse call traffic must never queue behind PACS image transfer or patient BYOD streaming. Vocera, Ascom Telligence, Rauland Responder 5, Baxter (Hillrom) NaviCare, and Cisco Webex Wireless Phone each have specific 802.11 fast-roaming and QoS requirements that must be aligned with the Wi-Fi controller before the nurse call system goes live.

Nurse call systems (Ascom Telligence, Rauland Responder 5, Baxter (Hillrom) NaviCare, Stryker Vocera Smartbadge, Cisco Webex Wireless Phone) often run their own dedicated Wi-Fi infrastructure or overlay on the hospital Wi-Fi with strict quality-of-service guarantees.

If the nurse call system shares the hospital Wi-Fi, QoS marking must be aligned so nurse call traffic never queues behind PACS image transfer. Stryker Vocera and Ascom Telligence badges in particular have specific 802.11 fast-roaming and QoS requirements that must be tested per design.

The design principle: PACS, HIS, and nurse call are workflow-critical clinical systems that Wi-Fi supports. Wi-Fi that "works" for laptops but degrades PACS retrieval by ten seconds has broken the clinical workflow. Post-deployment testing must include real clinical workflows, not just speed-test measurements.

What is a Typical Wi-Fi Refresh Timeline for an Indian Hospital?

A hospital Wi-Fi refresh for a 400-bed tertiary care facility runs 90 to 150 days from kickoff to steady state, phased around clinical calendar constraints. Elective surgery schedules, quarterly NABH assessments, and end-of-fiscal budget windows shape the timeline as much as any technical dependency.

Days 0 to 21. Discovery and Site Survey.

Predictive site survey using Ekahau AI Pro or iBwave Wi-Fi against current hospital floor plans, including drawn-curtain and open-curtain modelling for ICU spaces. Device inventory across biomed, clinical, admin, guest categories. Nurse call system integration mapping. PACS and HIS network path review.

Days 22 to 45. Design and Specification.

Access point count and placement finalised. Zoning architecture for IEC 80001-1:2021 segmentation specified. SSID plan (typically 4 to 8 SSIDs across biomed classes, clinical staff, admin, guest, digital signage, and nurse call). Firewall and inspection point placement. Cabling requirements for new access point locations, including RF-sealed pathway design for MRI rooms.

Days 46 to 75. Physical Rollout.

Cabling in first. Access points installed on schedule respecting clinical calendar (no drilling in operating theatres during scheduled surgery weeks). Switch upgrades where required for 2.5G+ uplinks. Firewall and controller commissioning.

Days 76 to 105. Cutover and Clinical Validation.

Zone-by-zone cutover from legacy Wi-Fi to new. Real-workflow testing with clinical staff, biomed devices, and nurse call systems. Radiologist workstation PACS retrieval testing. Roaming tests for patient monitors and nurse call badges.

Days 106 to 150. Hypercare and Evidence Generation.

30 days of hypercare with elevated support presence on-site. Evidence pack for NABH 6th Edition Information Management System (IMS) chapter compliance. IEC 80001-1:2021 risk file for medical device network zones. Handover to hospital IT and biomed engineering.

For larger hospital chains executing across multiple facilities, the pattern is a foundational architecture programme at one flagship facility (90 days) followed by parallel rollouts at subsequent facilities on 60-day cycles per facility, timed to each facility's operational calendar.

What Wi-Fi Evidence Do NABH and Insurance Auditors Ask For?

Under the NABH 6th Edition Accreditation Standards for Hospitals (mandatory for new applications from 1 January 2025), the Information Management System (IMS) chapter drives what assessors ask for on hospital IT and Wi-Fi. Assessors expect documented evidence across five areas: network architecture, medical device inventory, access control, incident management, and change control.

Network Architecture Evidence.

Current-state network diagram showing biomed zones, clinical zones, admin, guest, and inspection points. VLAN and SSID inventory. IEC 80001-1:2021 risk file with zone-by-zone rationale and responsibility assignments.

Medical Device Inventory.

Complete inventory of every network-attached medical device, with device class, biomed engineering owner, network zone, and last configuration change date. Reconciliation between the hospital's biomed engineering asset register and the network device discovery inventory.

Access Control Evidence.

SSID-to-user-population mapping. Authentication method per SSID. Access review evidence for privileged accounts on the network controller and firewall. Guest SSID access log retention aligned to CERT-In Directions (issued 28 April 2022) requirement of 180 days minimum.

Incident Management Evidence.

Register of network incidents affecting clinical operations in the assessment period, with root cause, remediation, and closure. Evidence of any medical device network security incidents notified to CERT-In within the 6-hour window and to the Data Protection Board under DPDP Rules Rule 7 (notified 13 November 2025) within 72 hours where personal data is involved.

Change Control Evidence.

Records of network changes affecting biomed zones, with joint sign-off from IT, biomed engineering, and (for changes affecting patient-facing clinical workflow) clinical operations. Aligned to the IEC 80001-1:2021 responsibility agreement.

NABH assessors will typically pick two or three specific past incidents or changes and ask for the full evidence trail. Preparation should assume the assessor will drill deep on any single area, not skim across everything.

What are the Common Mistakes in Indian Hospital Wi-Fi Design?

The six most common design mistakes across Proactive's Indian hospital Wi-Fi engagements in the last four quarters cluster in ceiling design, RF planning, SSID architecture, uplink provisioning, nurse call integration, and medical device segmentation. Each is remediable in a refresh cycle; the point of a design guide is to design them out at the start rather than rediscover them at the end.

Under-Designing MRI Room Coverage.

Assuming a corridor access point will reach into an MRI room. The Faraday cage prevents this. A dedicated in-room access point through the RF-sealed penetration is required.

Ignoring Curtain-Drawn ICU Conditions in the Site Survey.

Predictive site surveys done against empty ICU floor plans do not reflect operational reality. Drawn curtains change RF propagation significantly.

Using Guest SSID as a Catch-All.

Patient BYOD, staff BYOD, visitor devices, and even some clinical tablets end up on a single "guest" SSID with no bandwidth caps and no isolation. This degrades clinical traffic during peak visiting hours and creates a security-audit finding.

Not Accounting for Nurse Call System Wi-Fi Requirements.

The nurse call system arrives after the Wi-Fi is designed, and the roaming or QoS requirements don't match. Retrofit is possible but expensive.

Under-Provisioning Access Point Uplinks.

New Wi-Fi 6E or Wi-Fi 7 access points are throttled by 1 Gbps switch uplinks. 2.5 Gbps or higher uplinks are required to realise the access point's design capacity, especially in radiology reading rooms and high-density outpatient clinics.

Failing to Segment Biomed Devices per IEC 80001-1:2021.

Medical devices sit on the same VLAN as staff BYOD. This is the most common finding in hospital IT audits and a direct patient-safety concern in ransomware scenarios.

Frequently Asked Questions

Is Wi-Fi 7 deployable in Indian hospitals today?

Yes. Wi-Fi 7 access points from Cisco's Catalyst 9172, 9176, 9178, and 9179 series are commercially available in India, and DoT's January 2026 delicensing of the lower 6 GHz band (5925–6425 MHz) unlocks Wi-Fi 7's 6 GHz operation for Indian deployments. For hospitals planning a refresh in 2026, Wi-Fi 6E on Catalyst 9166I or Meraki MR57 remains the pragmatic default; Wi-Fi 7 on the 9172/9176/9178/9179 series is appropriate for flagship deployments where the ceiling design, cabling investment, and client ecosystem justify future-proofing.

Does Proactive design Wi-Fi that works in MRI rooms?

Yes. MRI-room Wi-Fi design requires a dedicated in-room access point fed through the room's RF-sealed cable penetration, with the access point positioned away from the magnet bore. Proactive's healthcare practice has delivered MRI-room Wi-Fi across tertiary care hospitals in India and has standard reference designs for 1.5T and 3T MRI installations, plus 7T installations at the research centres where they exist in India.

How does Proactive segment biomed devices per IEC 80001-1:2021?

Medical devices are placed in dedicated network zones (VLANs) with only the specific network paths their clinical function requires. Communication with HIS, PACS, and nurse call systems runs through inspected paths at a next-generation firewall. Cisco Cyber Vision (part of the Cisco Industrial Threat Defense architecture) provides device discovery and behavioural anomaly detection. Zone assignments and communication paths are documented in an IEC 80001-1:2021 risk file signed jointly by IT, biomed engineering, and clinical operations.

What evidence does NABH ask for on hospital IT and Wi-Fi?

Under the NABH 6th Edition Accreditation Standards for Hospitals (mandatory from 1 January 2025), the Information Management System (IMS) chapter expects network architecture documentation, medical device inventory reconciled to biomed engineering records, access control evidence per SSID and per user population, incident management records for the assessment period, and change control evidence for any network change affecting biomed zones. Evidence packs should be maintained continuously between assessments, not scrambled together in the month before the assessor arrives.

What's the typical timeline for a hospital Wi-Fi refresh?

A 400-bed tertiary care hospital typically runs 90 to 150 days from kickoff to steady state, phased around the clinical calendar. Multi-facility hospital chains typically start with a foundational programme at one flagship facility (90 days) and roll out to subsequent facilities on 60-day cycles per facility.

Why This Guide, From Proactive

Every hospital CIO we work with has the same problem: the Wi-Fi vendor's design guide is generic, the medical device vendor's requirements are prescriptive, and the NABH assessor's questions are specific. Proactive Data Systems has spent the last decade designing hospital Wi-Fi where those three constituencies meet, from single-facility private hospitals through pan-India tertiary care chains.

We are a Cisco Preferred Partner across five portfolios: Networking, Security, Collaboration, Data Center, and Services, with the Cisco Advanced Customer Experience Specialised designation. Founded in Delhi NCR in 1991. Over 1,500 enterprise customers across India. More than 100 certified engineers. A dedicated healthcare practice with implementations at hospital chains, standalone tertiary care facilities, speciality medical groups, and diagnostic networks across India.

When Indian hospital CIOs and biomed leads ask us to compare our approach to alternatives - a Wi-Fi vendor's direct professional services, a big-four consulting-led programme, or a generalist SI - three points typically decide the engagement. First, we design the Wi-Fi, the network segmentation, and the medical device zoning as a single integrated architecture, not as separate workstreams that later have to be reconciled.

Second, we carry Cisco specialisations across the full portfolio, plus current vendor familiarity with the Wi-Fi client ecosystem Indian hospitals actually run (GE HealthCare, Philips Healthcare, Mindray, BPL Medical, Stryker Vocera, Ascom). Third, our implementations produce evidence packs formatted for NABH 6th Edition assessors and biomed engineering leads, not just for the internal IT team.

We are not the only Cisco partner with hospital experience in India. Where a specific engagement demands a competitor's strength, a particular application specialisation, a specific vendor relationship, a distinct methodology, we say so. What we consistently do better than most is the join between Wi-Fi design, IEC 80001-1:2021 medical device segmentation, and NABH 6th Edition evidence generation, on a timeline that respects the clinical calendar.

If you are planning a Wi-Fi refresh, expanding a hospital chain into new facilities, or preparing for an NABH re-accreditation cycle, book a 30-minute conversation with a Proactive healthcare infrastructure architect. Not a sales engineer. Not an SDR. Someone who has delivered Wi-Fi for hospitals that look like yours and can defend the recommendations to your Medical Superintendent, your biomed engineering lead, and your NABH assessor.

To learn more about our solutions, write to us
at pro@proactive.co.in

www.proactive.co.in

PROACTIVE™
Enhancing Digital Experience