A network reference architecture for the evolving connected hospital

verizon business

Why read this paper?

This document provides a network reference architecture designed to support hospital leaders and decision-makers as they work to enable advanced and innovative operational capabilities in their healthcare facilities.

Fast-evolving technologies like AI, coupled with the expanding role of connected devices and Electronic Health Record (EHR) platforms, are dramatically increasing the need for network resiliency, security, speed, throughput and scalability within and around many hospitals. This paper provides detailed descriptions of the broad range of connectivity options available to hospitals and provides insights into how certain modes of wired and wireless connectivity are best suited for specific use cases.

Although this paper offers insights into how hospitals can optimize operations through the strategic deployment of new types of connectivity, it also advises on how to extract maximum value from legacy infrastructure investments.

Introduction: The evolving connected hospital

You've been hearing the hype about "the hospital of tomorrow" for years; at Verizon, we prefer to think of it as the "evolving connected hospital" – a community asset built on an integrated, secure, scalable and highly-available network that supports clinical systems, the hospital workforce, patients, visitors, and the ever-expanding healthcare vendor ecosystem.

As healthcare becomes increasingly digitized, hospitals have an opportunity – and an obligation – to reevaluate their current IT network strategy to ensure maximum operational efficiency and superior care delivery. The right mix of wired and wireless connectivity, deployed in the right locations for specific use cases, is necessary to support an ever-expanding ecosystem of mobile devices, Edge and Cloud computing, AI and the Internet of Medical Things.

Foundational capabilities and operational challenges

The evolving connected hospital offers more than the latest diagnostic breakthroughs and treatment options: it links providers throughout the facility, leveraging near real-time patient information, location data, asset tracking and immersive technologies to help provide the highest level of care possible. It is also designed to be as "future-proof" as possible, ready to support emerging solutions that will further enhance daily operations and improve clinical outcomes. In an evolving connected hospital, the following capabilities are foundational:

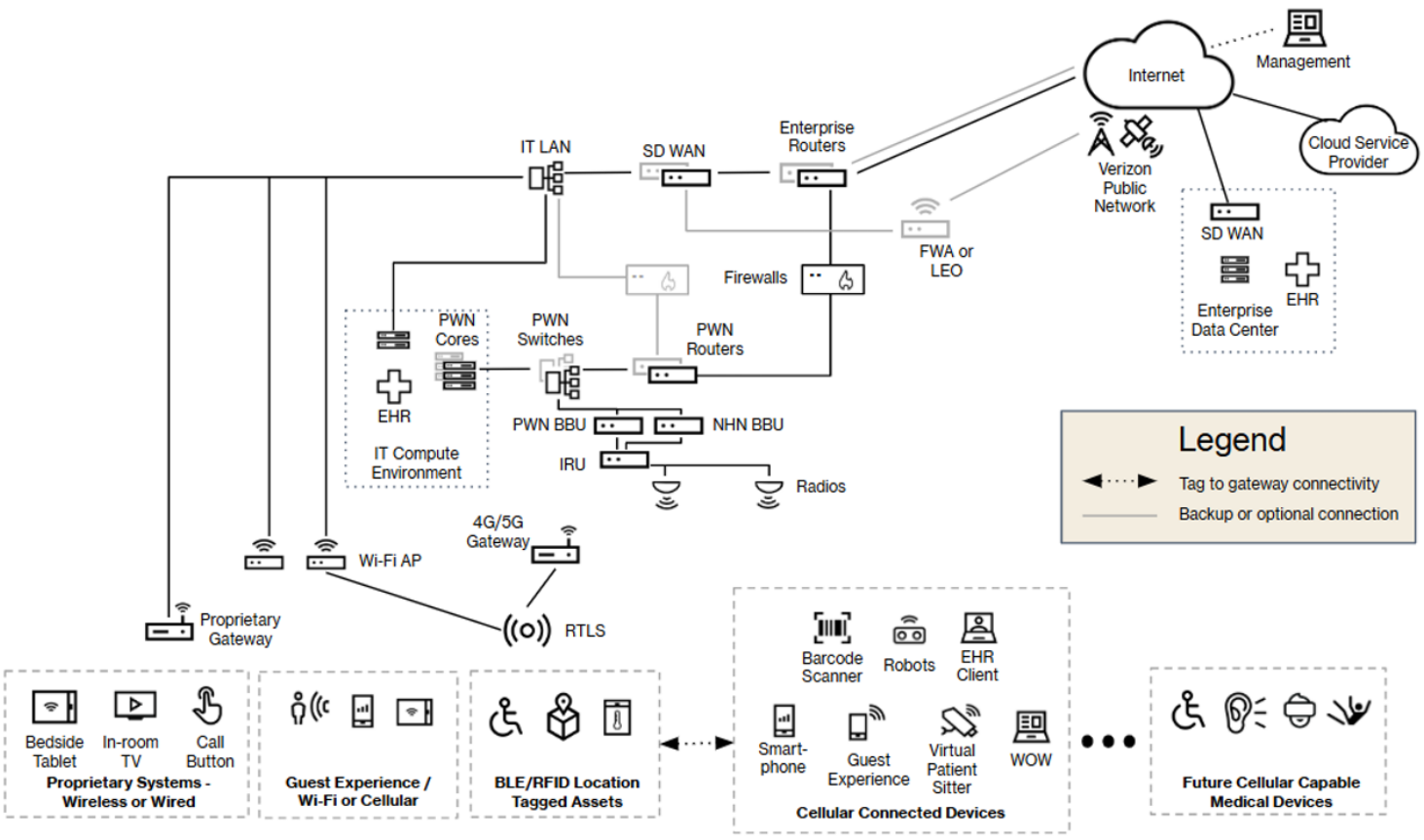
- **Near real-time patient monitoring**
  IoT-enabled wearables, sensors, and bedside devices constantly update patient vitals and alert staff to anomalies immediately.
- **Automated clinical workflows**
  Integrating AI with EHR systems reduces the time spent on administrative tasks, supports decision-making and diagnostic accuracy.
- **Optimized facility operations**
  Smart HVAC, lighting, and equipment usage systems can reduce energy consumption and maintenance costs while enhancing patient comfort and safety.
- **Business continuity and resiliency**
  Security events or unplanned outages taking down the enterprise network not only affect workflows but impact patient care. The ability to failover to an isolated cloud-hosted backup environment to maintain access to critical applications, primarily the EHR, allows healthcare institutions to maintain operations and potentially reduce the revenue impact.
- **Fully-leveraged medical device ecosystem**
  Secure, consistent wireless communications for mission-critical medical devices supporting clinical and operational functions such as software updates, calibration, and location and usage data.
- **Seamless roaming for mobile devices**
  Constantly on the move within the facility, healthcare professionals require uninterrupted connectivity as they move throughout the campus. This capability mitigates the risk of delays in accessing patient records, collaborating with colleagues, or communicating with patients.
- **Enhanced communication and coordination**
  Unified communications platforms connect physicians, nurses, and support staff across departments and locations and provide reliable access to public cellular networks to visitors and patients.

A number of challenges, however, can hinder progress toward developing these capabilities. They include:

- **Data silos hindering information flow:** The lack of efficient and effective connectivity across platforms creates data silos from legacy systems, vendor lock-in, and lack of interoperability.
- **Cybersecurity risks:** The adoption of digital technologies has increased exposure to ransomware attacks, data breaches, and other cyber threats, requiring complex security management across interconnected systems. The shift toward cloud-based EHRs and remote access necessitates more granular access control and constant threat monitoring.
- **Operational inefficiencies:** Inefficient workflows, poor resource allocation, and rising costs contribute to delays and sub-optimal care delivery. This includes underutilized medical equipment, bottlenecks in patient admissions, and manual reporting tasks that could be automated.
- **Complex and conflicting requirements for network services:** Demand for network bandwidth, speed and reliability vary widely by users and applications. Clinicians, patients, and visitors rely on a myriad of connected devices and integrated applications, each with their own requirements and expectations for service quality and performance.

Verizon has developed this reference architecture to help hospitals address these challenges.

High level reference architecture



The elements of the reference architecture

The following section describes key components of this reference architecture and offers insights for consideration when re-evaluating a hospital's network strategy and design.

Wired LAN and Structured Cabling

Robust and resilient wired LAN and switching infrastructure supports a diverse array of critical functions, from essential clinical systems to administrative operations, and acts as the nexus for all connected devices, both wired and wireless. Further, the LAN also serves as the bridge to external networks, allowing hospitals to connect to cloud services, remote clinics, and other healthcare partners, supporting seamless data exchange and collaboration.

Structured cabling (e.g., Cat6A or fiber) is fundamental to the wired LAN and switching infrastructure, acting as the physical medium over which all network traffic travels.

Wireless LAN (Wi-Fi infrastructure)

While Wi-Fi is widely adopted and simple for general enterprise use, its performance can be challenged by high device density, extensive coverage requirements, or applications demanding high bandwidth. Relying solely on Wi-Fi is becoming inadequate for the diverse needs of modern hospitals. A balanced approach leverages Wi-Fi for basic connectivity and deploys Private 5G (explained later in this paper) for more intensive, mission-critical applications. These technologies can enhance each other, building a resilient and versatile network.

Wi-Fi 7's full utilization of the 6 GHz band is a pivotal development. While Wi-Fi 6E introduced this band, Wi-Fi 7 fully leverages its potential with 320 MHz channels and advanced interference management. The 6 GHz band offers more than double the spectrum available to Wi-Fi 5 and 6, resulting in less crowded airwaves, fewer collisions, and significantly reduced interference. This provides a "clean slate" for high-performance, low-latency applications within hospitals, free from the legacy interference issues prevalent in the 2.4 GHz and 5 GHz bands. Effectively, this creates a dedicated, high-capacity wireless highway within the hospital, crucial for medical devices and real-time systems that cannot tolerate disruptions.

That said, even as Wi-Fi 7 offers improved bandwidth and latency, it doesn't eliminate the need for more access points (APs) in challenging radio frequency (RF) environments. The higher density of APs, due to Wi-Fi's shorter range, significantly increases costs related to installation, cabling, power, and maintenance, making it less ideal for sprawling and demanding environments.

Therefore, a hybrid approach, using Wi-Fi for less critical tasks and Private 5G for demanding clinical and administrative operations, is often the most effective solution. The ultimate decision should be based on a thorough assessment of a hospital's needs, applications, budget, and long-term digital transformation strategies.

Any connectivity disruption can severely impede clinical workflows and compromise patient safety. Thus, hospital Wi-Fi design and deployment must be built on four foundational pillars:

- **Performance:** Consistently delivering sufficient bandwidth, minimal latency, and high throughput for real-time applications and large data transfers.
- **Security:** Implementing robust measures like strong authentication, encryption, and network segmentation to protect sensitive patient data (ePHI).
- **Reliability:** Guaranteeing continuous connectivity through redundancy, seamless roaming, and effective electromagnetic interference mitigation.
- **Compliance:** Strict adherence to regulatory standards such as HIPAA, IEC 80001-1, and FDA guidelines is non-negotiable.

Patient and visitor Wi-Fi access

"Guest Wi-Fi" is routinely provided to patients, their caregivers, visitors and "non-staff" health care professionals and/or vendors working onsite. Designing Wi-Fi access for these constituencies in hospitals is challenging, requiring a balance between convenience for visitors and the imperative to protect highly sensitive patient data and critical medical infrastructure. A best-practice design adopts a multi-layered security approach beyond basic compliance to achieve cyber resilience. Key recommendations include:

- Rigorous network segmentation
- Robust authentication and authorization mechanisms
- Adoption of advanced Wi-Fi security protocols like WPA3 Enterprise

Operational best practices, such as comprehensive acceptable use policies and streamlined guest lifecycle management, are crucial. Additionally, Quality of Service (QoS) is critical to prioritize clinical traffic, and Wi-Fi infrastructure must be optimized for diverse healthcare use cases. Integrating network access with physical visitor management systems, continuous monitoring, logging, and auditing, combined with a proactive approach to regulatory compliance, forms the bedrock of a secure and adaptable guest access solution, supporting patient safety and operational integrity against evolving cyber threats. Later in this paper we discuss alternatives to Wi-Fi (including Neutral Host Networks) for certain use cases and capabilities, and provide guidance on security considerations for Wi-Fi.

Bluetooth low energy

Bluetooth Low Energy (BLE), a variant of the Bluetooth standard that trades off limited functionality in favor of extended battery life, has been used widely across the healthcare industry to support in-building location services such as wayfinding, asset tracking and patient monitoring.

The increasing adoption of wearable medical devices, patient monitoring devices and sensor technologies puts additional strain on legacy networks; the broad capabilities of these devices, their usage as a data transfer conduit to EHR systems, and new use cases coming online that leverage Bluetooth reinforces the need for network transformation.

Neutral Host Network

A Neutral Host Network broadcasts the public cellular signals from all three US mobile network operators (MNOs) and can be of great value to:

- Patients and their families, who need reliable connectivity to their personally-owned devices (which they use to access medical portals/EHRs and to call home/surf the web when they need to) without dependency on guest Wi-Fi. Poor connectivity can contribute to low patient satisfaction ratings.
- Hospital staff, who also need reliable cellular connectivity for their personal devices to feel connected to their families/outside world as needed. This helps with employee experience/engagement/retention in an industry where talent is hard to find and keep. Further, many clinicians working in a hospital are employed by other entities and use their own connected devices or devices not issued by that hospital.
- Vendors/third-parties, who operate within a hospital and need reliable connectivity to their devices, eliminating the need for hospital IT staff to provide access to their enterprise Wi-Fi environment.
- IT staff, because it provides a robust managed service, potentially reducing the cost and complexity related to managing aging Distributed Antenna Systems (DAS) which until Neutral Host Networks was the default approach to extend public networks indoors.[1]

Legacy DAS implementations typically have a shelf life of approximately ten years and are not future-proof. Many of the legacy DAS implementations currently in use are 4G only and are not upgradeable to 5G. Neutral Host Network implementations are typically less complex than legacy DAS and more in line with enterprise network solutions (e.g., standard rack space, fiber, CAT6 cable), often making them less expensive and less complex to implement, support and extend.

Medical device ecosystem connectivity via neutral host network

While Wi-Fi (802.11 standards) has historically been the primary choice for device connectivity, the evolving landscape of medical IoT demands greater reach, enhanced availability, and robust security. Consequently, device manufacturers are rapidly adding cellular connectivity and eSIM capabilities into their products, aligning with industry standards. This shift may help unlock the potential for advanced cellular features like network slicing to deliver guaranteed performance and isolation for critical medical applications.

Despite the undeniable benefits of connected medical devices, hospitals often meet requests for Medical Device OEM connectivity with caution. The complexities of network administration, the consumption of scarce IT resources, and the heightened security demands present significant challenges. Moreover, healthcare facility operators are keen to mitigate additional regulatory obligations under standards such as IEC 80001-1, FDA guidelines, and HIPAA.

Under IEC 80001-1, the Responsible Organization (typically the hospital) bears the ultimate accountability for the safe use and maintenance of the Medical IT Network (MITN) when medical devices are connected and operated via the hospital's IT network, including Wi-Fi. This means the hospital assumes responsibility for identifying, mitigating, and managing the risks associated with putting these devices on their network, which was historically managed by the device manufacturer.

For many networking needs, particularly those involving vendor partners or suppliers, the Neutral Host Network emerges as a valuable tool, as this approach offers several advantages:

- **Reduced hospital burden:** Hospitals avoid the direct costs and administrative overhead of providing and securing network services for external partners and their devices.
- **Enhanced security posture:** By leveraging cellular networks, hospitals can maintain clear boundaries, blocking unauthorized vendor equipment from connecting (or introducing risks) to their core networks. Partners can still be subject to audits of their security posture, penetration testing, and proof of liability insurance to maintain oversight.
- **Increased visibility and control:** Hospitals gain visibility into spectrum utilization and potential backhaul congestion. This enables informed decision-making without direct network management responsibilities for third-party devices.
- **Operational continuity:** By offloading certain third-party device connectivity to a separate, commercially managed cellular infrastructure, the hospital can reduce the impact of security breaches or ransomware attacks on its primary Wi-Fi and wired networks, contributing to greater business continuity.

Private Wireless Networks: a.k.a. “Private Cellular Network” (hospital-owned/provider-managed 4G/5G)

Private Wireless Networks that utilize 4G or 5G cellular technology significantly enhance hospital operations by delivering precise and pervasive cellular coverage, even in challenging environments. Key characteristics of a Private Wireless Network include:

- **High Performance:** These networks are architecturally designed for high performance, supporting massive device connectivity with high throughput and minimal interference.
- **Enhanced Security:** Private Wireless Networks are highly resistant to unauthorized access. Cellular spectrum is more difficult to locate and intercept than typical Wi-Fi signals. They offer a one-to-one mapping between the Subscriber Identity Module (SIM) and the device’s MAC address. When a SIM card is provisioned for a Private Wireless Network, it is assigned a specific range of IP addresses, enabling that device’s exclusive access to enterprise applications. Devices without a specific SIM configured for the private network cannot even detect its existence.
- **Future-ready and long refresh cycles:** The hardware for Private Wireless Networks is designed to support business needs for many years, offering a longer refresh cycle compared to other IT infrastructure or Wi-Fi. Continuous enhancements and operational fixes are provided through software updates.
- **Superior Reach:** Hospitals often have areas with spotty coverage due to complex RF landscapes saturated with electromagnetic interference from high-power medical equipment (e.g., MRI machines, electrosurgical tools), power distribution, HVAC systems, elevators, and fluorescent lighting. Private cellular technology, particularly LTE, offers superior signal penetration and reach to cover these difficult terrains.
- **Customizable Network Features:** These networks are highly configurable to meet specific operational and production needs, allowing for tailored performance for diverse applications.

Because of these characteristics, Private Wireless Networks are ideal for:

- **Business continuity and command and control:** In the event of a security breach or ransomware attack, many hospital CISOs may choose to disable their Wi-Fi network. A Private Wireless Network offers an attractive business continuity alternative, providing a resilient communication channel.
- **Medical imaging:** These units often require high-bandwidth access for reviewing and diagnosing large image files (e.g., X-rays, MRIs). Many of these units are now mobile, making wired connections impractical.
- **Video and computer vision applications:** New applications leveraging video and AI for continuous patient monitoring and alerting, require significant dynamic bandwidth. Private cellular is a superior option for evaluating and scaling these bandwidth-intensive use cases compared to existing 802.11 Wi-Fi, which is already managing a complex array of applications and Quality of Service (QoS) schemes.
- **MedTech partner connectivity:** For MedTech partners with pervasive networking requirements, often involving dedicated servers and even Ethernet cabling within the facility, private cellular offers an attractive alternative. It can provide defined SIM pools and network slicing capabilities to deliver architected wireless network performance, while remaining isolated from OEM and hospital network applications, enhancing security and management.
- **Robotics**: Many health systems are beginning to use robots / Automated Guided Vehicles (AGVs). Private cellular is less prone to coverage drops than Wi-Fi as the AGV passes between wireless access points.

The primary recommendation for transport is for the site to use two diverse Internet connections for primary and secondary connectivity. Leveraging SD-WAN, dual Internet access provides a flexible “smart” WAN which is capable of routing around packet loss and latency issues while providing encryption for corporate data. Direct Internet connections also allow for efficient connectivity to the cloud and other Internet based locations including the core networks of carriers participating in a Neutral Host Network. MPLS is an alternative for those companies that require an additional layer of security and reliability.

As a low cost way to provide additional redundant connectivity, Fixed Wireless Access (FWA) has become an attractive alternative, as it provides a separate way to connect a location that is not subject to local civil works and leverages completely separate infrastructure and technology. Where FWA is not available, Low Earth Orbit Satellite connectivity can be used to provide the same diversity advantages of FWA.

Network optionality and operational capabilities

The table below shows which capabilities are best enabled by which type of connectivity.

Connectivity type	Capabilities enabled by this type
Wi-Fi and Bluetooth Low Energy (BLE)	Asset tracking; front-office administration connectivity, guest and patient Wi-Fi; medical devices (heart rate monitors and glucose meters to wirelessly transmit health data); medication management and tracking
Neutral host	Patient-owned devices; “drop-in” visiting staff and vendor devices; patient room telehealth; hospital-wide Unified Comms
Private wireless	EHR workstations; tablets, smart phones; connected patient rooms; video for physical security, MedTech ecosystem devices; video and computer vision applications; medical imaging; robotics

Addressing security challenges with Zero Trust

The healthcare sector remains a prime target for cyberattacks, with system intrusions (including ransomware, phishing, credential theft and malware) constituting the overwhelming majority of attacks. Nearly two-thirds of all attacks come from external actors.[2]

Zero Trust Network Access (ZTNA) platforms can help address the security challenges that hospitals and healthcare organizations increasingly face. By adopting ZTNA, hospitals can:

- **Reduce the attack surface:** Limit access to only verified users and resources, thereby helping to mitigate the potential impact of security incidents.
- **Enable digital transformation:** Securely connect diverse systems, applications and users without compromising security or privacy.
- **Enhance compliance:** Meet industry regulations and data protection requirements through detailed access controls and robust security measures.
- **Improve operational efficiency:** Streamline workflows, simplify access management and gain valuable security insights to heklp optimize operations.

Important considerations for effective “Day 2” network support

Critical to successful operations is the clear articulation and regular publication of service level objectives and agreements. Objectives for various network types – Wired LAN, Wi-Fi, and Private Wireless – would be involved in these definitions, and these service levels should define key metrics such as availability targets, permissible maintenance windows, and time-to-repair for component failures. Consistent monitoring and reporting against these service levels ensure transparency and accountability, providing a benchmark for network performance and informing ongoing improvement efforts.

Other key elements of a robust network support capability include:

- **A comprehensive business continuity plan:** This plan should detail procedures for maintaining essential network services during outages, security breaches (e.g., ransomware attacks) and other disruptive events and should include a tiered escalation plan for outages.
- **An integrated network management system:** This system should provide centralized, near real-time visibility into the health and performance of all network components, including wired infrastructure, wireless access points, and cellular backhaul.
- **Continuous security posture monitoring and incident response:** This includes regular vulnerability assessments, penetration testing, and adherence to regulatory obligations under standards such as IEC 80001-1, FDA guidelines, and HIPAA.
- **Employee and vendor access management:** A robust system for screening, approving, and credentialing network management system access for both employees and vendors is fundamental.

Conclusion: Paving the way for the future of healthcare delivery

The network reference architecture described herein provides a comprehensive roadmap for hospitals aiming to thrive in the increasingly digitized healthcare landscape. By strategically integrating robust wired and wireless infrastructure, adopting advanced security measures like Zero Trust, and leveraging solutions like Private Wireless Networks and Neutral Host Networks, hospitals can overcome current challenges and unlock new opportunities. This proactive approach ensures the network is not just a utility, but a foundational, life-supporting system.

Embracing this architectural vision will empower healthcare organizations to build truly resilient, secure, and scalable "evolving connected hospitals," ultimately delivering superior patient outcomes and helping to shape the future of medicine.

Learn more

Verizon stands ready to partner with hospital executives and IT leaders to leverage this reference architecture as a starting point for discussions about network optimization.

For more information please contact your Verizon Account Manager or visit verizon.com/business/solutions/industry/healthcare/

Verizon Business contributors in alphabetical order:

Kevin Donahue
Lee Field
Thomas Fuerst
Robin Goldsmith
David Grady
Jeffrey Granvold
Taru Jain
Kevin Kitagawa
Ahmed Moussa
Greg Taylor
Peter Tomfohrde

1. Up to 50% lower CapEx, up to 70% lower OpEx, and upto 70% lower power consumption. https://na.experiences.ericsson.net/neutral-host-solutions
2. “Verizon 2025 Data Breach Investigations Report” https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf