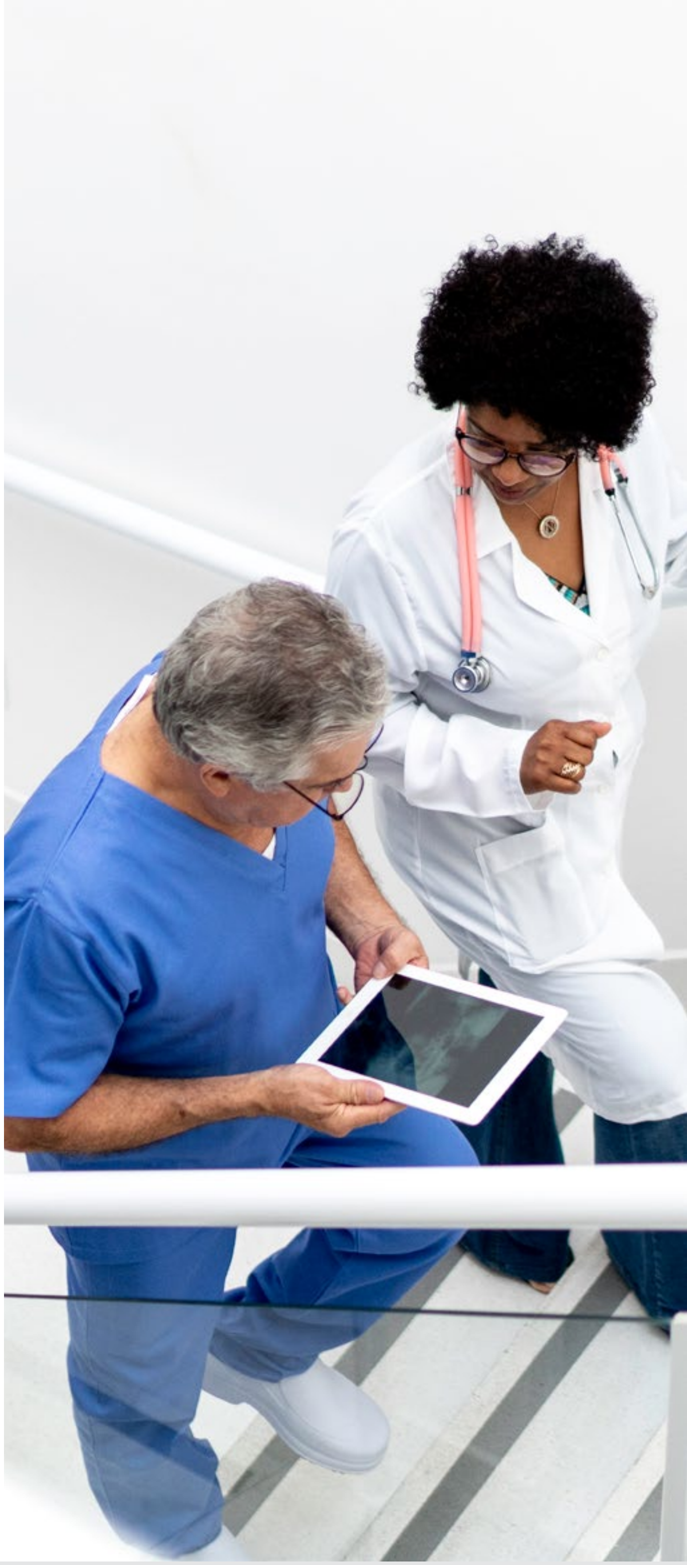
Networks for the Future of Healthcare

ciena

Contents



1. Introduction

The healthcare industry is undergoing a fundamental shift from the traditional siloed care delivery model in which patient data is not widely shared among providers, clinicians, and patients. In the new care-delivery model, stakeholders across the full spectrum of healthcare providers share, adopt, and apply data and medical expertise in real time. Some industry pundits have dubbed this new model the "real-time healthcare system."[1]

This shift is being driven primarily by patients, who are accustomed to the conveniences of digital experiences received from other industries like retail and financial services. Healthcare systems are beginning to realize that they need to treat patients more like consumers. This includes providing real-time access to doctors, clinical information, and online engagement with their care team. The ability to capture, aggregate, and share patient data and actionable information across the entire ecosystem of healthcare providers is key to delivering a more consumer-driven treatment model.

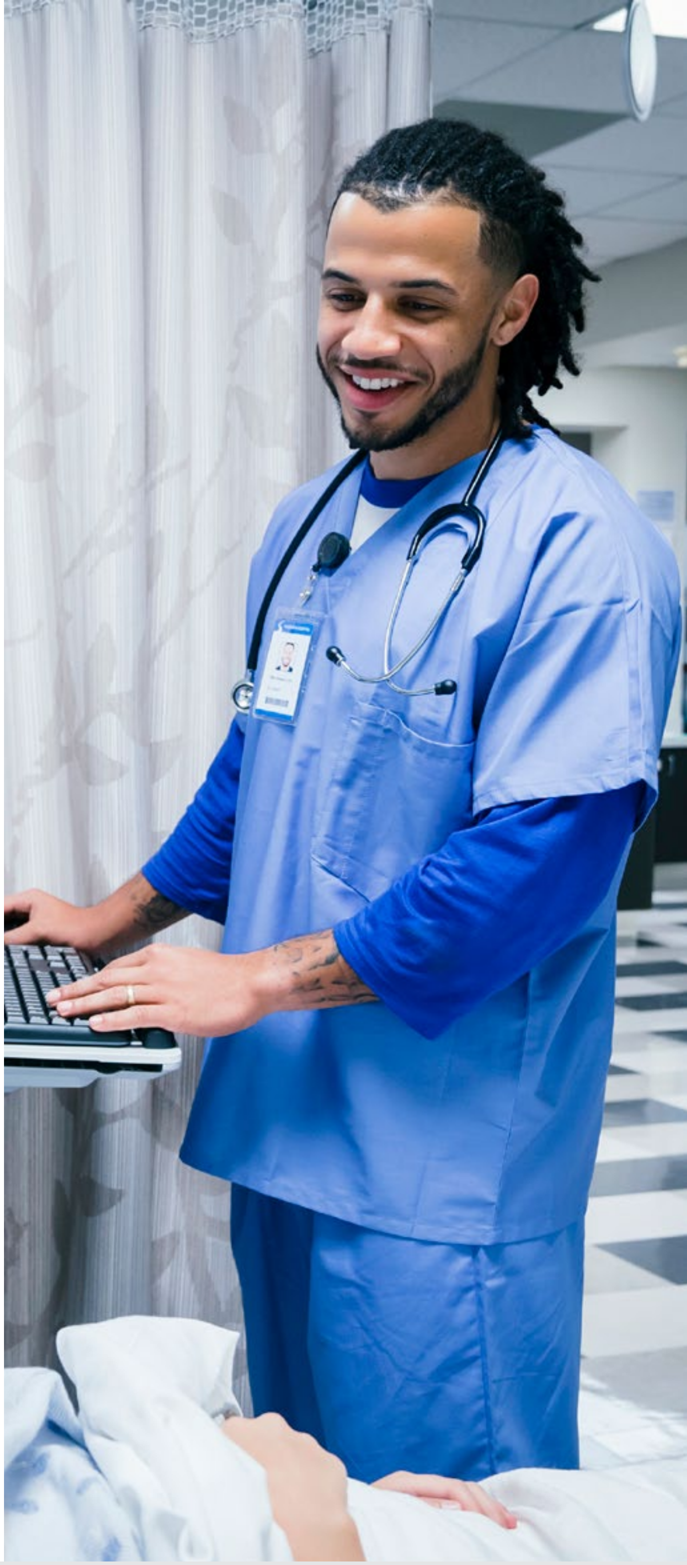
The global pandemic helped drive the shift to a more collaborative, real-time care delivery model by accelerating the adoption of online virtual medical consultations between patients, providers, specialists, and hospitals. In addition, healthcare systems gave employees greater flexibility to work from home. The proliferation of virtual healthcare visits, video-based collaboration between providers, and 'work-from-anywhere' arrangements will continue for the near future.

The communication network is a critical foundation to the success of this new collaborative, real-time healthcare delivery model. By combining communication technologies with new digital healthcare applications, providers can more effectively coordinate patient care and optimize the patient experience whether in a virtual, physical, or hybrid environment. Healthcare staff also require secure, 'anytime, anywhere, any device' connectivity to patient data and digital applications, irrespective of where they are working. In addition, healthcare remains a top target of cyber thieves, and the cost of a data breach is higher in healthcare than in any other industry.[2]

Healthcare systems are therefore prioritizing the enhancement of their networks to make them more flexible, secure, resilient, and adaptive to meet the increased demands of the new digital healthcare delivery model—and to ensure the long-term success of the business.

This eBook provides insights on the network requirements to support healthcare technology (HealthTech) and to accelerate digital transformation—making real-time clinical collaboration a reality.

- Trends driving digital transformation in healthcare
- Digital healthcare applications driving network decisions
- Impact on healthcare system networks
- Requirements for networks supporting real-time healthcare systems
- Ciena's experience building healthcare networks



2. Trends driving digital transformation in healthcare

- **Consumerization of healthcare:** Retail and financial services customers have become accustomed to the convenience of real-time access to online transactions, people, and services from any location and any connected device. When dealing with healthcare providers, patients expect this same level of real-time, online engagement and connectivity to their healthcare provider team. To better compete for patients, healthcare systems are seeking to provide a more consumer-like experience through new digital medical applications.

- **Competition:** New digital-only entrants, nationwide pharmaceutical chains, and some big-box retail stores are now offering various healthcare services. Many traditional healthcare systems view these new market entrants as a more serious competitive threat than other traditional healthcare providers. But some innovative healthcare systems seek to cooperatively compete with new entrants, leveraging their capabilities to lower the cost of care and better connect with patients.

- **Virtual collaboration:** Many healthcare providers are leveraging video and online collaboration tools to work with providers outside their ecosystem. One example is tele-ICUs—which extend critical care resources to the bedside, regardless of where the hospital is located. Another example is radiology operations command centers, which can remotely train, guide, and assist less-experienced colleagues in remote satellite facilities. Similarly, interventional physicians can leverage virtual collaboration platforms to provide remote peer-to-peer guidance and assistance in medical procedures.

- **Cybersecurity:** According to the most recent Ponemon Institute report, the average total cost of a data breach in healthcare increased from $7.13 million in 2020 to $9.23 million in 2021.[3] The large range of sensitive data included in healthcare records—combined with the proliferation of connected medical devices and the variety of healthcare providers accessing patient data—make healthcare a top target of cyber thieves.

3. Digital healthcare applications driving network decisions

The trends listed in the section above, plus the evolution towards providing more personalized healthcare, are driving healthcare systems to invest in digital transformation. The 2022 Healthcare Information and Management Systems Society (HIMSS) State of Healthcare Report reveals that over three-fourths of U.S. healthcare systems believe that investing in digital transformation is very important.[4] The innovative technologies and applications included in digital transformation initiatives may differ by healthcare system, but typically include the following:

- **Artificial intelligence:** AI is increasingly being deployed in healthcare, with 77 percent of clinicians either currently using some form of AI or expressing interest in doing so in the future.[4] Radiologists leverage AI to perform redundant tasks, eliminate bias-based reading errors, identify data patterns in images, and enhance workflow processes.
- **Real-time medical analytics:** Large healthcare systems are harnessing analytics platforms that combine systems engineering, predictive analytics, and problem solving to manage patient flow while aiming to preserve clinical quality, safety, and the patient experience.
- **Natural language processing:** These solutions can generate accurate medical notes as the provider conducts a medical consultation with the patient.
- **Mixed reality:** Interactive and immersive technology can help medical students learn faster, enable surgeons to map out surgical plans on a patient, and assist patients in understanding the procedure they are about to undertake.
- **Streaming video:** In-hospital, real-time video-streaming use cases include centrally managed remote patient monitoring for fall reduction, surgical monitoring for collaborative procedures and teaching, safety programs against baby abduction risk, Alzheimer patient containment, and monitoring of drug dispensing areas.
- **Connected medical devices:** A typical large hospital has 10 to 15 connected medical devices per bed. The bandwidth-intensive and low-latency requirements of some of these devices are driving many hospitals to deploy 5G.
- **Smart building systems:** Connecting heating, cooling, lighting, and other environmental and security services to an automated network manager maximizes comfort while reducing costs.

These are just some of the new digital applications available to healthcare systems. In the post-pandemic world, they will become increasingly essential to the efficient operation of any healthcare organization, from individual practices to hospitals to research facilities. One common feature of all these diverse digital healthcare applications is that they generate enormous volumes of data. The healthcare industry generates far more data than any other industry.

The following statistics summarize trends in U.S. healthcare technology:

Today, approximately

30%

of the world's data volume

is generated by the healthcare industry.

By 2025, the compound annual growth rate of data for healthcare will reach **36%**[5]

Hospitals produce

50

petabytes of data per year[6]

A single patient generates up to

80

megabytes annually

in imaging data
and electronic medical records[7]

The volume of healthcare data generated by medical applications needs to be stored, analyzed, secured, and shared across a wider range of stakeholders collaborating on patient treatment.

4. Impact on healthcare system networks

The network can also be considered the backbone of the entire hospital system, as telehealth tools, smart beds, devices that monitor vitals, electronic health records (EHRs), Picture Archiving and Communication Systems (PACS), smart tablets, and more, need to be connected to function properly.

Healthcare networks are often constrained by statically configured network islands that are isolated or stitched together with inefficient connectivity and managed by multiple management systems. There is often no automated ability for the network to adjust to sudden fluctuations in demand, such as a mass-casualty incident or operation of multiple bandwidth-intensive applications occurring on the same day.

As healthcare systems shift towards a more real-time data sharing capability and deploy more bandwidth-intensive and latency-sensitive digital applications, the network may become strained beyond its capacity. As a result, the healthcare industry is experiencing more instances of network congestion and unplanned outages. Poor network performance and outages can cause failures that can have a cascading effect on multiple digital healthcare applications, which severely impacts clinical operations throughout the healthcare system. Unplanned downtimes can be costly. According to a recent report, outages can cause healthcare facilities an average of $208,600 in immediate lost revenue.[8] And, as more medical devices and digital applications come on to the network, maintaining network uptime becomes critical to ensure quality patient care.

As healthcare enterprises move to real-time data sharing capability, they need more flexible and agile networks. They also need more efficient and cost-effective solutions to connect smaller healthcare sites, as well as secure internet and mobile connectivity to enable remote monitoring and telemedicine.

5. Requirements for networks supporting real-time healthcare systems

When determining network requirements, architects and planners need to balance capacity requirements, latency sensitivity, and density of locations that need to be connected. They need to determine 'peak-time' network bandwidth needs and forecast future capacity requirements. Most importantly, network architects and planners need to strike a balance between under-architecting and over-architecting the network. Under-architecting the network will cause more congestion and unplanned outages that will impair application performance. Similarly, the network should not be over-architected with costly bandwidth capacity that is not fully utilized, especially during 'off-peak' hours.

The following sections can help healthcare network architects and planners determine the optimal network architecture for their current and future needs:

- Bandwidth requirements
- Distribution and traffic patterns
- Connectivity options
- Encryption
- Other considerations

5.1. Bandwidth requirements

When planning network capacity, it is important to consider all traffic sources and traffic patterns. Most hospital systems run clinical applications, administration systems, billing and revenue assurance programs, radiology, medical research, surgery centers, and teaching hospital applications on the same network, often at the same time.

Hospital system use cases that drive network bandwidth include:

- Patient admissions and discharge
- AI-assisted radiology
- Diagnosis and virtual collaboration
- Application access for visiting clinicians
- Robot and virtual-assisted surgery
- Medical teaching and research
- Guest and staff Wi-Fi
- Networked medical sensors and devices
- Smart building systems, including climate control, energy, and security

The radiology department is typically the biggest consumer of bandwidth within a healthcare system. As hospital radiology departments shift to 3D medical imaging, the number of image sets and file sizes grow substantially.

- Digital breast tomosynthesis images can range from 450 MB to 3 GB[9]
- Each Computerized Tomography (CT) scan data set can reach 20 GB to 30 GB in size
- An average cardiac MRI exam today is about 200 MB, while a ViosWorks exam is about 20 GB

Other bandwidth-intensive digital healthcare applications include genomic sequencing, next-generation EHRs, mixed reality, and high-resolution video. Other applications are not as bandwidth-intensive but add to the daily network requirements. During operational 'peak times,' all applications and functions are consuming bandwidth at the same time. If the network lacks sufficient capacity, congestion and outages occur.

5.2. Distribution and traffic patterns

In ordinary circumstances, bandwidth requirements are primarily driven by a highly digital approach to healthcare delivery, which varies between healthcare systems. Contributors to bandwidth and network requirements include:

- Number and type of sites: Headquarters campus and data center, affiliated physician offices, outpatient centers, rural clinics, research centers, and data centers
- Distances between facilities
- Peak number of patients, clinicians, staff, visitors, and others concurrently accessing the network
- Adoption of digital and virtual collaboration, 3D imaging, type of electronic medical record platform, connected medical devices, and mixed-reality surgical and learning technology
- Use and mix of cloud-based IT administrative and office solutions
- Adoption of mobile devices by clinicians, staff, patients, and visitors—laptops, tablets, smartphones, and others
- Projected growth in users and application traffic

5.3. Connectivity options: What is the best network?

Wherever possible, fiber-based connectivity is the best choice for healthcare systems. Fiber provides the highest capacity, lowest latency, and most reliable connectivity.

Fiber-based connectivity can be provided in several diverse ways:

Private network

Healthcare systems have two options when considering a private network:

- The first option is to procure fiber-optic cables, deploy them underground or along utility poles, and then deploy the packet-optical network switches to light the fiber. Healthcare systems also must have experienced IT staff to maintain the fiber and manage network operations.
- The second option is to lease dark fiber from a service provider. With dark fiber, the service provider owns and maintains the fiber, but the healthcare system owns and manages the packet-optical switching equipment used to light the fiber. Some dark fiber service providers may agree to bundle the network equipment within the dark fiber lease contract.

Some healthcare systems may deploy their own fiber cables or private 5G, especially for intra-campus networks. For Wide Area Networks (WANs), the majority find that leasing dark fiber is the best choice for systems that need to quickly scale from 10 Gb/s to 100 Gb/s. The growing availability of dark fiber, along with innovations in packet-optical networking technology, has made a private network much more attractive.

Dark fiber is usually leased from a service provider for an extended period—often 20 years. Dark fiber pricing and availability vary widely from area to area. In some markets, affordable dark fiber may be plentiful, while in others, it might not even be available.

To drive down costs and ensure the highest data transmission rate possible, healthcare systems opting for dark fiber networks should choose converged packet-optical platforms. These innovative network platforms provide the flexibility to support multiple services, future demands, and various protocols on a common infrastructure. These converged packet-optical platforms combine high-performance Layer 0/1 optical switching capabilities and comprehensive Layer 2 Ethernet switching capabilities in a single platform, with a common administrative interface.

Converged packet-optical networks can help contain capital expenditure by collapsing network layers and consolidating equipment; they can also contain operational expenditure by unifying provisioning and management functions and reducing recurring energy and rack space costs. The ability to transport and dynamically prioritize multiple traffic types is critical to providing the rich digital learning environment students and staff demand. The addition of Dense Wavelength Division Multiplexing (DWDM) allows for the transport of more data across the dark fiber, helping to maximize return on network investment.

Managed services

In this use case, the hospital system leases fiber-optical capacity from a telecom service provider that is shared by many other customers for a recurring monthly fee. The service provider owns and maintains the fiber-optic cabling as well as the equipment used to light the fiber. A managed service offering is the simplest option to deploy and manage interconnecting hospital locations, outpatient and rural clinics, data centers, and affiliated physician offices. It is often the best choice for hospital system locations requiring 100 Mb/s to 10 Gb/s WAN capacity. Service providers offer a variety of lit fiber options, including managed Ethernet private line services and managed optical wavelength services.

Managed service offerings provide several key advantages, including:

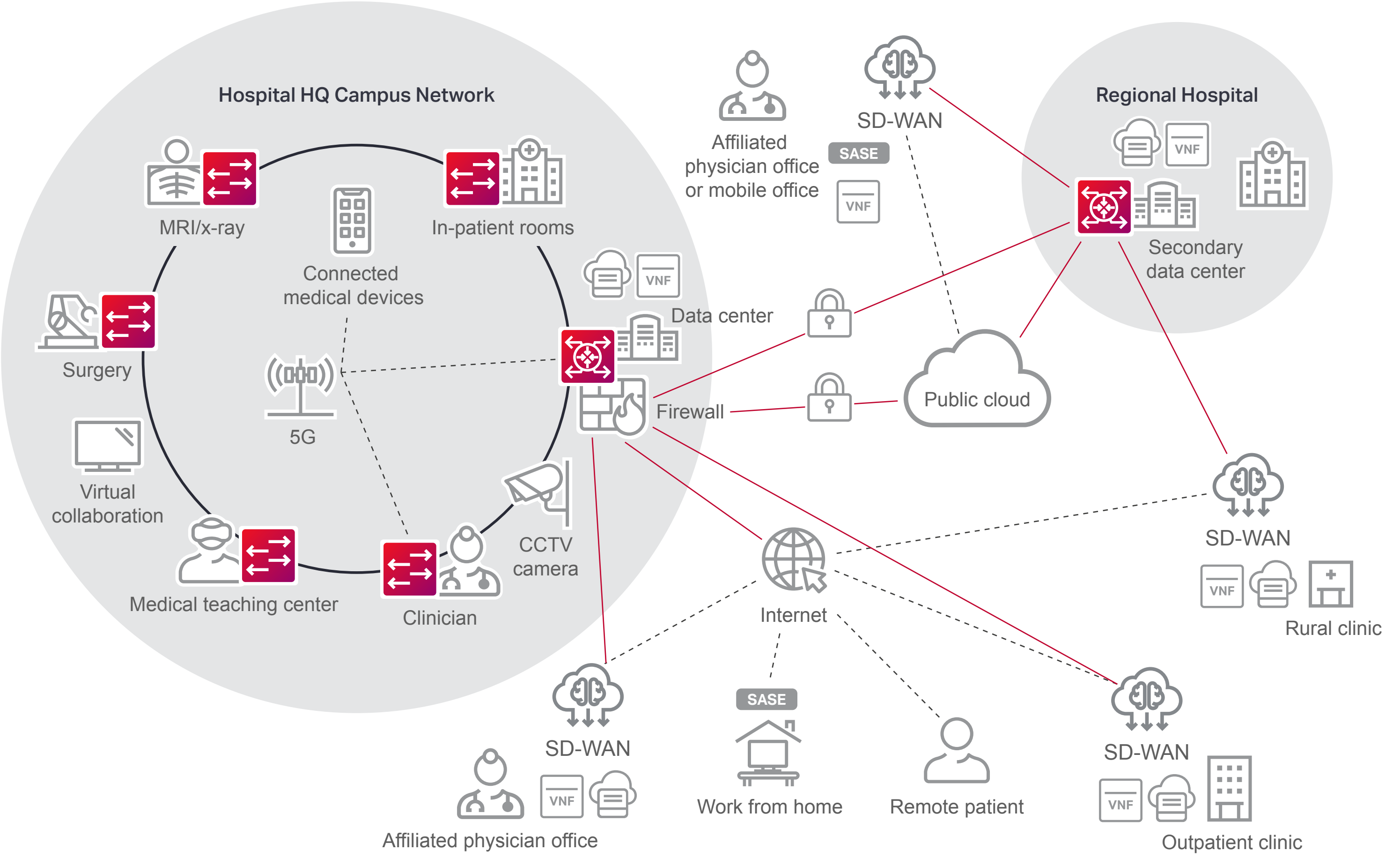
- **Services provider responsible for end-to-end connectivity for services** ('single hand to shake') with a full managed service
- **Lower in-house skills required** at hospitals and clinics
- **Shorter time-to-connect** as the service provider assumes responsibility for enabling all aspects of connectivity
- **Easier to upgrade** because capacity or feature upgrades can often be enabled through software configuration
- **Better overall performance** as the service provider will be in the best position to ensure end-to-end network performance

Data security

Healthcare has been a top target of cyberattacks because their networks contain many types of information—from proprietary medical research data to information about patients' personal lives, financial records, and health. Hospital systems employ multiple security standards to safeguard their networks and must comply with federal HIPAA and state regulations. Failure to secure protected health information can result in significant financial penalties, remediation cost, reputational damage, and patient churn. Encrypting 'in-flight' data across the network, deploying physical or virtual firewalls, adopting a 'zero-trust network access' (ZTNA) approach and securing 'work-from-anywhere' endpoints are security features that hospital systems should consider.

Hospital system network architecture

The image below depicts a typical multi-region hospital system network configuration.



Hospital campus network

This network configuration includes connectivity between diverse functions within different buildings (for example, radiology, surgery, teaching hospital, admittance, and discharge) and the administrative headquarters/primary data center. The connectivity could be via fiber optics for ultra-high bandwidth needs such as PACS in radiology, or via 5G.

Hospital system core network

The hospital system headquarters and primary data center connects to one or more regional headquarters throughout a state or multiple states. As many healthcare systems have opted to continue private premises-based or hybrid cloud strategies, the on-premises data centers house enormous volumes of data and applications. This approach means that the healthcare systems must maintain robust disaster recovery and business continuity approaches that include secondary, tertiary, and public cloud-based data centers.

Typically, these secondary, tertiary, or cloud-based data centers are located at a sufficient distance to serve as ‘active/active’ data mirroring and backup for disaster recovery and business continuity purposes. The connectivity between headquarters, the primary data center, regional headquarters, secondary, tertiary, and cloud data centers can be via 10 Gb/s to 100+ Gb/s dark fiber, managed dark fiber, managed wavelength, or 100 Gb/s Ethernet services.

The data centers can replace numerous physical application servers with a single high-end compute device that supports multi-tenant, virtualized application workloads. Connectivity to internet service providers and public cloud providers typically involves 10 Gb/s or 100 GB/s circuits.

To ensure privacy and security of protected patient data in transit between these locations, hospital systems can add network-level encryption. To comply with HIPAA and state data security standards, the National Institute of Standards recommends encryption at the Advanced Encryption Standard 128,192- or 256-bit encryption for electronic protected health information.

One Ciena multi-facility hospital system client upgraded its core network from 1 Gb/s to 10 Gb/s to support the bandwidth needs of new healthcare applications deployed throughout the system. This included a new remote emergency room patient video monitoring application, which decreased annual emergency room mortality rates by 40 percent.

Hospital system WAN

The headquarters campus and each regional headquarters connect to numerous affiliated physician offices, outpatient treatment centers, rural clinics, and other facilities. With the growing popularity of Software-Defined WAN (SD-WAN), these smaller locations can now split network traffic between Ethernet and internet underlay connectivity services to improve application performance and reduce cost. For example, a small site could leverage SD-WAN capabilities to route non-mission-critical network traffic over a business internet service, while more mission-critical, latency-sensitive traffic could be routed over the 1 GigE or 10 GigE Ethernet service.

Advances in SD-WAN services now provide customers the choice of deploying a SD-WAN solution via a dedicated physical device or as a software-based, virtualized version uploaded onto a universal Customer Premises Device (uCPE). Typically, a healthcare facility that opts for a uCPE solution will add other Virtual Network Functions (VNFs) from ‘best-of-breed’ vendors, such as virtual router, virtual firewall, virtual load balancer, and others. For those healthcare locations that prefer to subscribe to these types of services from a single vendor, some SD-WAN vendors are bundling a virtual router and firewall with the SD-WAN service.

One Ciena healthcare system customer replaced physical routers, firewalls, and other devices with VNFs across all existing and new affiliated physician offices. By eliminating the need to manually replace physical devices at each location, the customer estimates it will save three million dollars.

To deliver a better ‘consumer-like’ experience to patients, healthcare systems will continue to offer virtual consultations, healthcare visits, and monitoring over video-based collaboration platforms. This connectivity will typically be via business internet access for the healthcare provider, and residential internet access for the patient. In addition, ‘work-from-anywhere’ arrangements will continue for the near future. However, remote access points to headquarters applications often can increase vulnerability to cyber data breach. Remote and mobile employees require a cloud-based suite of security functions to enforce a ZTNA policy and protect against data breach. Services such as Secure Access Service Edge (SASE) provide a bundle of such cloud-based security services that, in addition to ZTNA, also include cloud access service broker, firewall-as-a-service, secure web gateway, remote browser isolation, data loss prevention, and others.

Some healthcare workloads that combine AI with other applications involve large sets of structured and unstructured data that need to be accessed in as close to real time as possible to enable critical clinical decision making. For these types of applications, healthcare systems are beginning to deploy edge compute solutions that speed data delivery and decision making to enable providers to deliver a better patient outcome. Edge compute solutions can include virtualizing multiple applications onto a single high-end compute device with a robust software stack that supports multi-tenant workloads via application integration and service chaining.

5.4. Other requirements

In addition to connectivity and bandwidth, several other factors should be considered, as shown in Table 1, below.

Consideration	Impact
On-demand capability	Crucial to support dynamic bandwidth needs, including normal peak and non-peak periods, online testing for teaching hospitals, and emergency situations with a mass influx of patients. Networks should be designed with flexibility and adaptability in mind.
Network resiliency	Network connectivity is crucial to ensure 'always-on' access to digital healthcare applications and patient data. As patient records are primarily digital and applications are becoming more latency sensitive, congestion and outages can impact application performance and hospital staff's ability to provide quality patient outcomes.
Manageability	'Single-pane-of-glass' operations are key to ensuring manageability of network and service lifecycle, including service assurance, fault management, and ongoing optimization.
Security	Ensuring privacy and security of protected health information is paramount to ensuring compliance with HIPAA requirements. Data-security technologies such as end-to-end network encryption, physical or virtual firewall, ZTNA, and others can defend against data breach and help avoid the financial and reputational consequences.
Scalable for future needs	HealthTech evolution will drive new requirements: edge compute, distributed cloud, virtual machines, and technologies yet to be defined. These will continue to drive the convergence of connectivity, compute, and security, and accelerate digital transformation in healthcare.

5.5. Operational considerations

Networks typically consist of technologies and solutions from multiple vendors. This can result in complex 'swivel-chair' operations—where different operations teams need to access different operating and support systems to plan, provision, and assure services. This operational complexity can make it slow to diagnose and resolve issues. Worse, operations staff may not even be aware of issues until the customer calls.

'Single-pane-of-glass' operations is key to ensuring effective manageability of all aspects of network and service lifecycle—from service creation, modification, assurance, and fault management, through ongoing optimization.

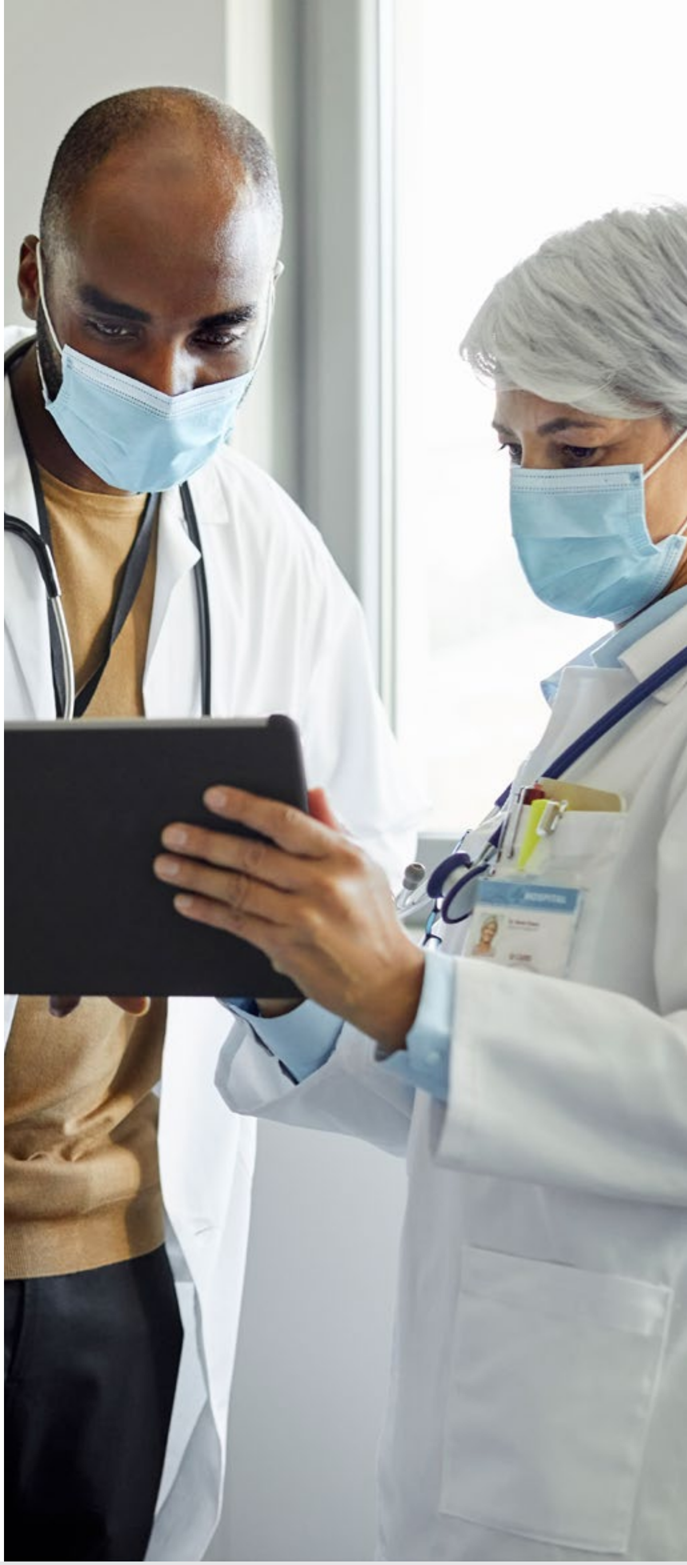
Different models exist in transitioning to simplified operations, including:

- Utilizing an umbrella operations environment such as an orchestrator or domain controller to unify operations across vendors
- Utilizing a single vendor across all network domains

There is no 'right' answer, but operational efficiency should be a primary concern when designing networks in support of HealthTech.

Outsourcing ongoing network operations

Many hospital systems do not have the resources and skills to fully manage a private network. Staffing an in-house operations team can be expensive and time consuming. As a result, many systems turn over network operations to a trusted third party. Multi-region healthcare systems might consider outsourcing some or all their network operations to a qualified vendor. Acting as a virtual member of a healthcare system's IT team, the vendor can remotely monitor and control the private network—helping to identify, isolate, and resolve issues quickly and efficiently.



5.6. Recommendations

For both hospital systems and service providers, the key is to be adaptable. It is not possible to foresee what the future in HealthTech will bring, but hospital CIOs and service providers can prepare for it.

For healthcare systems, new tools and ways of teaching will drive changes. Deploying a private network that can adapt to changing needs is essential.

- **Grow with demand:** Architect the network to be able to meet peak-time' needs while maintaining the scalability to support future capacity requirements. Avoid under-architecting the network and impacting application performance. Similarly, avoid over-architecting the network with costly bandwidth capacity that is not fully utilized, especially during 'off-peak' hours.
- **Flexible traffic flows:** As multi-region hospital systems move from a hub-and-spoke model to a more collaborative or peer-to-peer model that includes SD-WAN, enabled network traffic routing over diverse underlay connectivity services ensures the network provides the topology and flexibility to accommodate changes.
- **Integrity:** Networks should be configured with infrastructure and process reliability, and backup connections, backup sites, and operational integrity should be verified; consider how onsite-to-cloud–based operations may be impacted by network integrity.
- **Security:** A network must be encrypted, secure, and support 'zero-trust' to protect patients, providers, and staff.
- **Features:** Requirements may change over time; simple service add-ons (such as firewalls or IP VPN services) may evolve to necessitate things like VNFs and edge compute, so ensure the network can accommodate these possibilities.

For service providers, infrastructure that can evolve with hospital requirements is essential:

- **Bandwidth growth and flexibility:** Be accommodating of bandwidth growth; provide tools such as 'bandwidth on demand' to allow healthcare CIOs flexibility as their needs change.
- **Flexible with connectivity:** Traffic patterns are changing based on healthcare technology adoption, so be flexible accommodating change; allow for tools like 'service on demand' and be prepared to accommodate fast service turn-up and change.

- **High reliability:** For healthcare technology, many network features that were once a luxury are now a necessity, so delivering high-reliability features (dual site, dual link, operations processes) with matching Service Level Agreements (SLAs) is a key differentiator.
- **Analytics and visibility:** Employ tools that can aid in service and network visibility; for example, analytics can be utilized to monitor changing traffic patterns and proactively adjust services before users are impacted.
- **Security:** Offer tools and processes to protect patients, providers, and staff by providing options for encrypted connections, private networks, core and edge protection, and 'work from anywhere,' as well as tools and services to assess security risk.
- **Flexibility in contracting:** Make it easy for healthcare customers to evolve their services; 'on-demand' network capability should be matched with flexibility in business contracts.

Ciena has proactively partnered with the healthcare and hospital community for decades. This collaboration helps drive research and development for the evolution of packet-optical and virtualization networking technologies, helping to develop the digital healthcare networks of the future.

A converged packet-optical solution from Ciena provides a scalable, flexible, high-capacity transport of transit and protects traffic—from 3D medical imaging to AI training sets and next-generation EHRs—to support the changing demands of the digital healthcare community.

[1] Healthcare IT News, “The Real-time Health System: Adapting Healthcare to the New Normal”, Jul 2020

[2] IBM, “Cost of a Data Breach Report 2021”, 2021

[3] HIMSS, “2022 State of Healthcare Report”, 2022

[4] HIMSS, “2021 Future of Healthcare Report”, 2021

[5] RBC Capital Markets, “The Healthcare Data Explosion”

[6] Frontiers in ICT, “Better Patient Outcomes Through Mining of Biomedical Big Data”, Dec 2018

[7] Fierce Healthcare, “82% of Healthcare Organizations have Experienced an IoT-focused Cyber Attack, Survey Finds”, Aug 2019

[8] HelpNet Security, “Data Breaches and Network Outages: A Real and Growing Cost for the Healthcare Industry”, Mar 2021

[9] Trachtman, Les, Purview, “PACS Requirements for Digital Breast Tomosynthesis (DBT), 3D Mammography, and Molecular Breast Imaging (MBI)”, Oct 2016