GUIDE

Supporting today's data-intensive clinical environments

Technology is transforming all aspects of today's healthcare, from care delivery to administration. Create a network that adapts to rapid change.

Here's step-by-step guidance for planning a network infrastructure that will help you advance your digital health initiatives and improve efficiency and patient outcomes.

An era of rising expectations

When patients engage with your healthcare facility — whether in person, by phone or video link — they expect at least two things: a positive experience and confidence they are receiving the highest quality care.

Along with advanced equipment and knowledge, data has emerged as an essential tool for delivering quality healthcare and improving patient outcomes. Electronic health record (EHR) systems, digital imaging, telehealth, patient portals, remote monitoring, the Internet of Things (IoT) and big data initiatives have made secure, reliable, high-speed and low-latency connectivity a must in today's complex and bandwidth-intensive clinical environments.

The ability to access vast amounts of business and clinical information is key to ensuring patients receive individualized care while the health system continues to operate efficiently. This access to vital information also presents a challenge, placing new expectations and demands on your network and digital health infrastructure.

This guide will help you prepare to meet the network infrastructure requirements of the digital healthcare environment for today and tomorrow.

Inside this guide

Spectrum ENTERPRISE™

Step 1

Identify your needs

1 **Identify your needs**

2 Evaluate owned vs. managed services

3 Choose the right partner

1 2 3

Step 1: Identify your needs

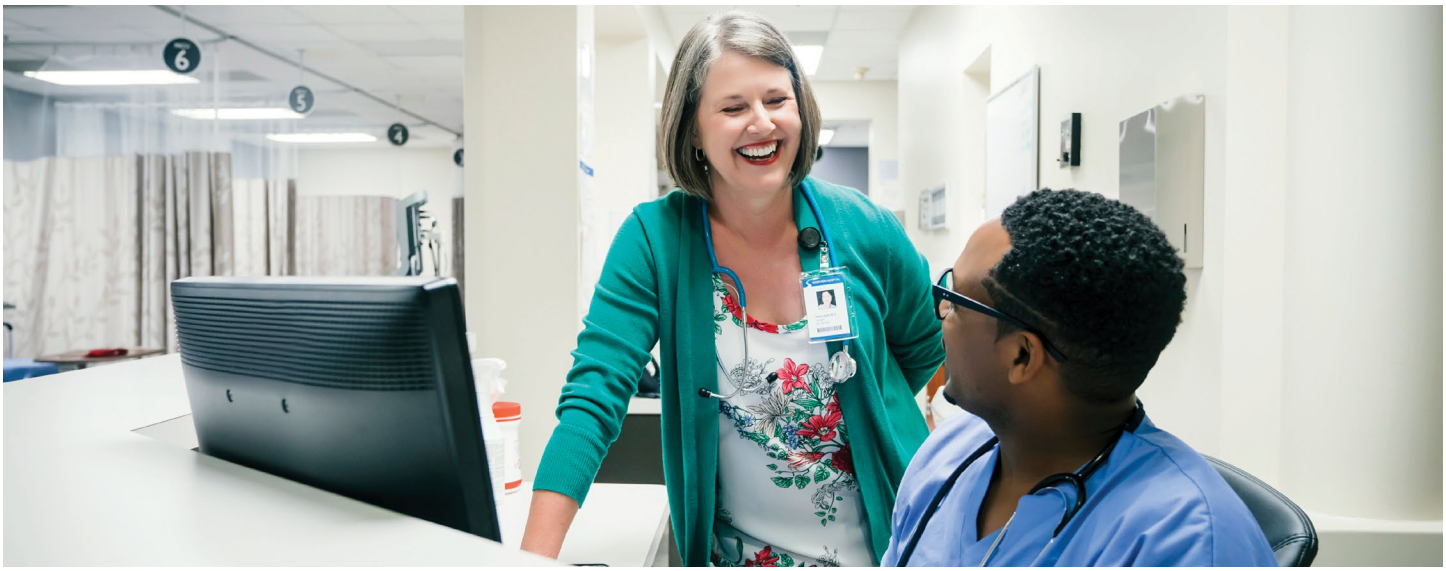
In healthcare, having fast, reliable and continuous access to data literally saves lives. It also serves as the foundation for achieving the Quadruple Aim of healthcare: (1) Improving population health in a (2) cost-effective manner, while improving the (3) patient experience and (4) clinician experience across the continuum of care.

Making smart network decisions today can deliver:

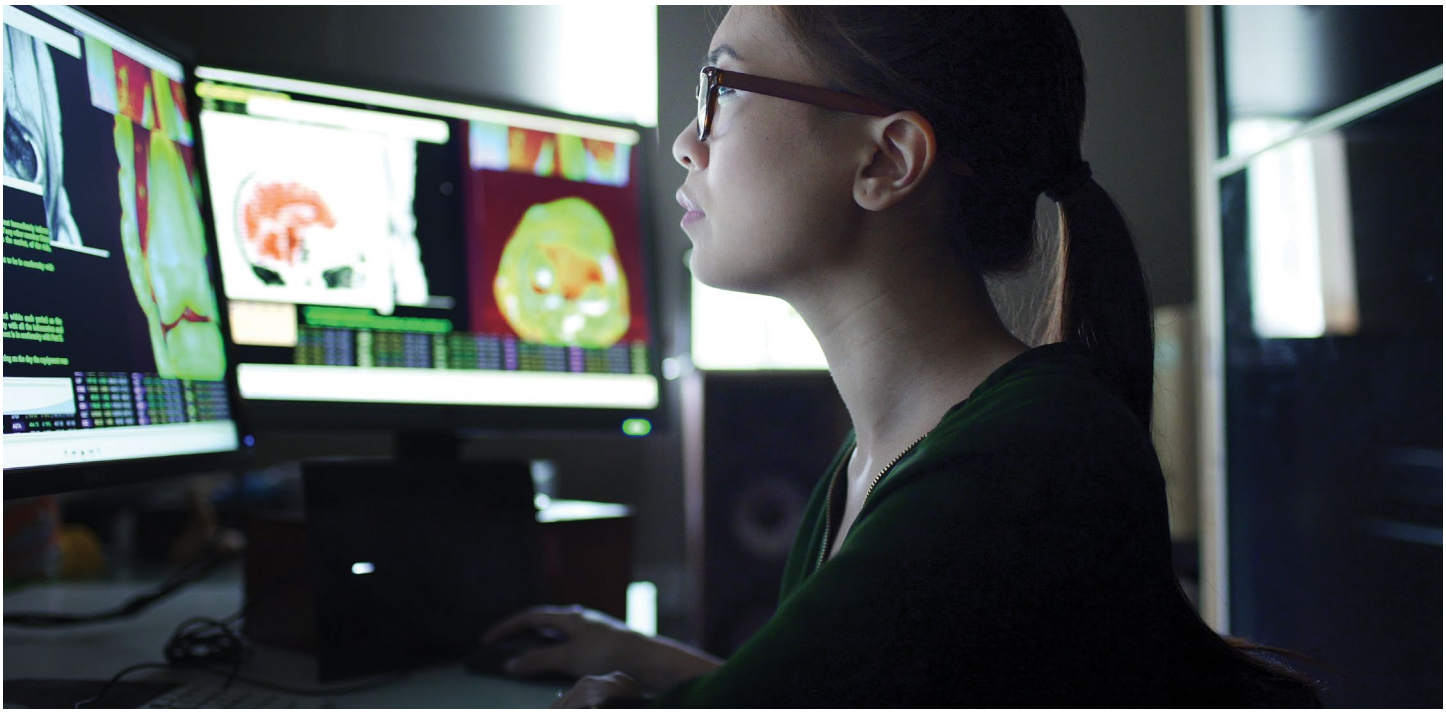
- Improved population health outcomes through coordination of care, prevention and personalized medicine.
- Lower costs through smarter use of resources and greater efficiency.
- Better patient experiences through seamless and thereby less stressful interactions with providers and hospitals.
- Better clinician experiences through reliable, streamlined systems that help them focus on patients.

Of course, the key to all of these benefits is ensuring that your healthcare facility has reliable, high-speed connectivity that can scale to support evolving data, networking, voice and security needs.

To assess your overall connectivity needs, ask what you will require from your network over the next three-to-five years. Aspects to consider include the amount of bandwidth you'll need, your wide area network (WAN) infrastructure, your WiFi coverage and protection to keep your network secure.



Spectrum ENTERPRISE™



Bandwidth: The lifeblood of all healthcare connectivity

With the increase of Internet of Medical Things (IoMT) and the need to share large imaging files, bandwidth demands are constantly rising. Here are some factors to consider when determining your bandwidth needs:

User base: *How many simultaneous users will you have?*
With potentially hundreds of users needing high-speed internet connectivity, determining your specific needs — and allowing for growth — is essential because each additional user will directly impact bandwidth requirements. Also consider how many cloud-based applications you use and how your staff interacts with the Web.

Capacity: *What's the volume of imaging files you need to transfer?*
With improved imaging technology and the extensive use of the picture archiving and communication system (PACS), transferring large diagnostic image files has become common. Clinicians who need immediate access to files containing hundreds of megabytes of data can't afford to wait minutes for a download. Think about your own facility's use of imaging files to ensure you have sufficient bandwidth to increase staff productivity and provide positive patient experiences.

Streaming video: *Do you currently offer or plan to offer telehealth video consultations?*
HD video allows for better communication, giving providers more detailed patient images. Keep in mind that HD video may require up to three times more bandwidth than SD-quality video.

Spectrum ENTERPRISE™

New devices and applications: *How will you leverage IoT devices, patient portals and emerging network-based applications?*
The explosive growth of sensor-based devices and connected applications has increased the demand for digital connectivity. Along with this, more and more facilities are providing patients with convenient, 24/7/365 access to personal health information and care management via patient portals.

Take action

Know your bandwidth usage
Use a network monitoring tool to understand how much of your capacity is being used at various locations throughout the day. Usage report data will help you understand key trends, such as peak usage times, sources of bottlenecks and how much bandwidth individual applications use. This tool can help your determine how much more bandwidth you'll need to achieve your goals.

WAN: Seamlessly connect all your locations

The WAN of the future is highly agile, scalable and adaptable, capable of expanding to meet your organization's ever-changing needs. It should be customizable, with features to optimize performance and the intelligence to identify problems. As you evaluate your WAN's readiness for the future, here are some key questions to guide you.

Capacity: *Does your network have the capacity to meet users' needs now and into the future?*
Consider how many users you'll have (including providers, staff, patients and visitors), applications they use, clinician mobility devices and how many IoT devices will be connected to your network over the next several years. Will your bandwidth meet expected demand? What latency is appropriate between network sites? You need a network that won't become congested during peak usage times.

Spectrum ENTERPRISE™

Resiliency: *Is your WAN designed with failover protections to withstand a cut line or other outage to a critical network connection?*
Loss of a network connection can be extremely disruptive to a digital-dependent care environment without sufficient backup capabilities. Building a resilient, reliable network involves planning for the worst with alternate routes available for your network traffic.

Flexibility: *Can your network easily accommodate changing needs?*
Does your network infrastructure give you the flexibility to easily make adjustments, such as adding new locations? An agile network gives you more control, allowing you to respond quickly to changing needs.

Visibility: *Can you see data traffic patterns and application usage across your network?*
To make smart policy decisions based on network performance, you need to see what's going on with your network at any given time. Having both real-time and historical insight into your network operations allows you to monitor performance and set or adjust policies as needed.

Having real-time and historical insight into your network performance lets you make smart policy decisions.

Efficiency: *Does your network include features designed to maximize the efficiency of data flow?*
Features such as traffic shaping allow you to prioritize certain types of network traffic (like communication and clinical applications) over other types (such as video streaming), resulting in faster and more reliable network performance.

Take action

Consider the advantages of SD-WAN
Healthcare providers seeking greater network utilization and simplified network management over distributed locations should consider the advantages of a managed, software-defined WAN (SD-WAN). A managed SD-WAN service allows for application-aware routing while reducing network complexity and bandwidth cost. In addition to offering centralized network monitoring, visibility and control, as a managed service, it comes with the support of a skilled partner to design, deploy, implement, manage and monitor the solution.

WiFi: Continuous access enhances clinician mobility and patient experience

Fast and reliable WiFi coverage throughout a medical campus is essential to enable patients, clinicians, staff and visitors to use technology effectively. Consider these items as you determine your wireless needs:

Multi-tenancy: *Does your WiFi infrastructure allow you to create separate, secure wireless networks from shared access points?*
A key challenge in creating wireless environments is establishing separate networks for clinicians, patients, visitors and IoT devices using the same WiFi access points. The latest WiFi technology lets hospitals and health systems enjoy better network security and efficiency while also lowering the cost of WiFi deployment with less radio frequency (RF) signal interference.

Spectrum ENTERPRISE™

Total network demand: *How many people will use your WiFi network?*
The number of network users you anticipate should include clinicians, patients and administrative staff, as well as visitors. Consider how on-site community events or clinical seminars may affect your network. Are you able to accommodate temporary bandwidth spikes?

IoT: *Have you factored in IoT devices?*
Organizations are gathering real-time information from an increasing array of devices, sensors and applications. The significant growth in the IoT market is attributed to the need for cost-containment, rising focus on patient engagement and increased patient-centric care delivery. According to IoT Analytics, it is expected that by 2025, there will be approximately 27 billion connected IoT devices.[1]

Self-optimization: *Does your WiFi infrastructure contain built-in intelligence that continuously looks for ways to optimize performance so users receive the best experience possible?*
Innovative WiFi technology can improve network performance in congested, high-density environments (such as common areas) by dynamically changing the channel selection, channel width and transmission power of RF antennas to match user needs. Automating this process reduces signal interference and results in a better wireless experience for clinicians, staff, patients and visitors.

Load balancing: *Does your WiFi infrastructure automatically distribute users evenly to prevent network congestion?*
Dynamically transferring users between network access points, in real time, as they roam the medical campus results in better signal performance for each user, even in large crowds.

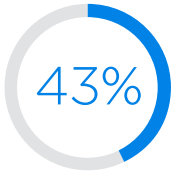
Spectrum ENTERPRISE™

Seamless failover: *Does your wireless network have the ability to switch users over to another access point seamlessly (and automatically) in the event of a failure, so service continues uninterrupted?*
Today when an access point fails, it's possible for another to automatically pick up the user session with no drop in service. If access points are configured in clusters, then standby paths are created in real time to alternate devices within the same cluster. During high-priority sessions (such as voice or video use), these sessions are synchronized so if a network device fails, switching the user to another network device is seamless. Users don't experience service disruption and IT staff aren't burdened with complaints or help requests.

Take action

Conduct a site survey
Designing a wireless environment can be complex. Healthcare leaders have to account for possible signal interference, as well as how walls and building materials affect the range of wireless signals. This can be especially challenging in hospitals. A site survey done by an experienced provider can help you plan for adequate coverage.

Network security: Protect patient information and your reputation



of health industry executives cite cyberattacks as a serious risk to their organization.[2]

Cybersecurity and privacy are vital concerns in healthcare. Providers must not only ensure that they are protected against malicious hackers, but also that all networks, processes and IT systems meet stringent federal regulations and HIPAA requirements. Having a powerful, high-speed and highly scalable network does no good if the network is paralyzed in an attack. As you assess your security needs, here are some key considerations:

A firewall with unified threat management (UTM): *Can you administer and manage multiple security functions from a single console?*
A firewall solution that combines intrusion detection and prevention features, antivirus software, deep packet inspection, application layer control and advanced security reporting within a single product can simplify network security while saving time and money. With fewer devices to configure and maintain, network administrators can have protection while also achieving a single, holistic view of network threats.

DDoS protection: *Can you protect your network from a Distributed Denial of Service (DDoS) attack?*
In a DDoS attack, multiple computers target a single server, overwhelming the server's network with traffic so it cannot respond. DDoS attacks are fairly easy to carry out and can be very disruptive to health systems, which have become increasingly popular targets. The best defense is to deploy a cloud-based security solution to intercept malicious traffic before it reaches your network.

Vulnerability testing: *Are you regularly scanning your network for potential weak spots that can be exploited by hackers?*
As a general rule, you should test your network on a quarterly basis to find and correct possible weaknesses in your security defenses. Ideally, this testing should be performed by a certified third party.

Spectrum ENTERPRISE™

Healthcare organizations must react to changes quickly by making their network as automated as possible.

HIPAA-compatible: *When planning a network upgrade, make sure that the configuration of your network solution facilitates your ability to meet the HIPAA requirements for system availability, disaster recovery and redundancy.* For security, think about designing your network so that your network data doesn't touch third-party networks, and backhauling all internet access through a central site with filters. If any of your networks failover onto the public internet, ensure that data remains encrypted through AES256 VPN tunnels.

Other best practices: *Have you adopted other industry-recognized best practices for keeping your network secure, such as network segmentation?* Segmenting your network involves separating groups of systems or applications from each other either physically or virtually. This limits communication between various systems, which limits how much damage a hacker can do on your network.

Take action

Perform a security audit

A network security audit can help you understand where your network might be vulnerable to possible security breaches. A security audit identifies all of the assets on your network and whether their operating systems are up to date. It also reviews the configuration of your firewall and assesses the biggest risks to your network security so you know which threats are the most important to address.

Reliability and latency: Ensure rock-solid performance

Network reliability and latency — key measures of network performance — have critical significance in a healthcare environment. Today's connected healthcare networks support numerous applications, processes and devices that deliver essential services to patients and providers. Real-time and interactive health applications (such as patient monitoring and video consultations) demand low latency.

Spectrum ENTERPRISE™

Network is the foundation on which connected healthcare is built — bringing together all aspects of individual care, from initial outreach of patient to provider through to care of patient and post-care follow-up.

Achieving a reliable, low-latency network involves intelligent selection of multiple components — including carrier transport services, protocols, switches, routers and firewalls — working together to deliver optimal, assured performance. As you plan the evolution of your network, here are some questions to bear in mind.

Connectivity: *What is the right transport media?*
Selecting the right transport media will have a significant impact on your network reliability and latency. Fiber offers higher bandwidth, lower latency over long distances and resistance to many of the problems that can affect other transport types. For example, fiber is not affected by interference from nearby power lines or high voltage electrical equipment, it can withstand wide temperature fluctuations, and it can be submerged in water. These are key features to think about when considering connectivity that is used to support business continuity and disaster recovery.

Direct connectivity: *Should you deploy a private network?*
For improved reliability and predictable latency between sites on your WAN, private and directly-connected networks are preferred. Fiber-based Ethernet eliminates performance concerns that can occur with other technologies. Likewise, consider establishing a private-cloud connection if you're using a cloud service provider (e.g., AWS or Microsoft Azure) for your enterprise applications.

Take action

Identify and eliminate single points of failure
As you examine your network, look for vital devices or pathways that lack failover protection. One way to ensure that your network isn't exposed to issues or failures is to build diversity into your network. Network diversity ensures that alternative paths are available for network traffic in the event of a failure. That way, a disruption in the primary line won't impact your overall business continuity.

Spectrum ENTERPRISE™

Step 2

Evalute owned vs. managed services

1 Identify your needs

2 **Evaluate owned vs. managed services**

3 Choose the right partner

1 2 3

Step 2: Evalute owned vs. managed services

Network solution options available to healthcare providers have evolved rapidly over the last decade to provide greater efficiency and cost savings. Hospitals, health systems and their affiliates no longer have to own and manage their own routers, firewalls, wireless access points and other network technology; instead, they can choose a solution that is fully owned, installed and managed by a service provider.

Although purchasing and managing network equipment yourself might appear to be cheaper, there are hidden costs and risks of which you need to be aware. Here are key factors to consider when weighing this decision.

Reliability. *Have you budgeted for maintenance and repairs?*
Keeping things running smoothly might require constant tweaking and firmware updates. When you own your network equipment, you're responsible for all maintenance and repairs. How might this affect the reliability of your network? With a managed solution, you have the peace of mind that comes from having a service-level agreement (SLA) in place guaranteeing network uptime and issue resolution response times.

Staff expertise. *Do you have skilled network technicians who can maintain and troubleshoot your network?*
If so, then it might make sense to own your own infrastructure. If not — or if you'd rather have your in-house experts focus on more strategic projects — then a fully managed solution may make more sense, where support teams are available to monitor equipment, troubleshoot problems and deploy technicians 24/7/365 if problems arise.

Flexibility. *Does it make sense to invest in a specific network infrastructure with a fixed capacity?*
If your needs change faster than you anticipate, or if you underestimate the demands on your network, you'll need additional capital to make changes. If flexibility is a priority, a managed solution lets you add capacity as needed and offers you access to the latest equipment as technology evolves.

Budget model. *Would you rather incur a large upfront expense or have monthly recurring charges?*
Some healthcare providers opt for a single capital outlay to buy and install their own network equipment. Others find that a fixed monthly fee for a managed service makes budgeting easier. Keep in mind that owning your own equipment means you'll need to set aside funding for maintenance and upkeep, which can add up quickly.

Spectrum ENTERPRISE™

Step 3

Choose the right partner

1 Identify your needs

2 Evaluate owned vs. managed services

3 **Choose the right partner**

1 2 3

Step 3: Choose the right partner

Your choice of service providers matters. You want a company that is not just a technology vendor, but a partner who understands healthcare organizations and is fully invested in your success. The right partner can help you at every step in your project, ensuring you make the right network decisions to advance your digital health initiatives.

Here are four important qualities to look for in a network service provider:

Advanced technology. Does the provider employ the latest standards and technologies? Do the company's products reflect the latest industry developments?

Industry leadership. Does the provider have the size, capacity and expertise to serve your needs effectively? Is the company stable and reliable, with a strong reputation in the industry?

Experience in the healthcare market. Does the provider understand the unique needs and goals of healthcare professionals? Does it have a proven track record of success in serving the needs of clinicians, administrators and patients?

High-quality service. Does the provider value you as a customer? Does it have U.S.-based call centers backed by local support experts to provide prompt answers to your questions? Is someone available at all hours in the event of an emergency?

Spectrum Enterprise — your partner in transforming healthcare

The selection of your service provider matters. Spectrum Enterprise is more than a technology vendor. We are an experienced and engaged partner that is fully invested in your success.

Spectrum ENTERPRISE™

Spectrum Enterprise serves more than 119,000 healthcare organizations nationwide.

Spectrum Enterprise offers a complete array of connectivity solutions — from Fiber Internet Access (FIA) and WAN services to managed WiFi and security — to simplify healthcare IT management and eliminate the need for a patchwork of providers. Our dedicated IT healthcare experts, exceptional network performance, end-to-end accountability, responsiveness and support has made Spectrum Enterprise the partner of choice for over 119,000 healthcare organizations nationwide.

Spectrum Enterprise is committed to meeting your connectivity and communication needs to help ensure quality patient care and efficient facility operations. We give you the agility to stay ahead of fast-changing healthcare trends through a comprehensive range of services that include:

Fiber Internet Access: Achieve dedicated internet connectivity with symmetrical upload and download speeds and bandwidth up to 100 Gbps.

Wireless Internet: Provide primary or secondary internet access over LTE Advanced technology with this all-inclusive wireless internet service.

Wireless Internet Backup: Experience automatic wireless internet failover and failback service that is managed for you.

Ethernet Services: Meet ever-growing data needs by connecting locations with a fast, reliable wide area network (WAN) solution backed by a SLA and built on a dedicated fiber infrastructure. Bandwidth up to 100 Gbps is available.

Cloud Connect: Extend your network with fast, secure and dependable private cloud connections to cloud service providers.

Managed WiFi: Meet patient, provider and staff demands for reliable connections to the internet with ubiquitous coverage across your facilities and 24/7/365 support.

Enterprise Network Edge: Improve the network experience for your teams when scalability, performance and flexibility are paramount to your business. Powered by Fortinet, the solution simplifies IT operations by providing SD-WAN and security in a multi-cloud-ready platform that brings together connectivity, equipment and network management to support both hybrid networks and workforces.

Managed Network Edge: Simplify the deployment and management of your network with this modular, all-in-one solution. Delivered over the Cisco Meraki platform, the solution offers security, routing, SD-WAN, WiFi, switching, environmental sensors and smart cameras. Achieve flexibility and scalability with connectivity, equipment and network management from a single partner.

Managed Router Service: Efficiently route traffic and improve bandwidth use without investing in hardware or day-to-day management.

DDoS Protection: Guard against malicious volumetric attacks designed to overload your network and prevent access to applications, systems and information with world-class DDoS threat identification and mitigation.

Spectrum ENTERPRISE™

Making critical technology more affordable for rural healthcare providers

If you're a rural hospital network or healthcare provider, dedicated Spectrum Enterprise experts can help you take advantage of federal funding programs that can reduce the cost of network technology investments to enhance patient care.

The Rural Health Care (RHC) Program, established by the FCC in 1997, helps public and non-profit rural healthcare systems improve the quality of healthcare through enhanced connectivity via two sub-programs.

With the Healthcare Connect Fund, eligible providers can receive up to a 65% discount on an array of communications services. The Telecommunications Program funds the difference between the rural and urban rates for telecommunications services.

For additional details and information on the RHC Program and how Spectrum Enterprise can help, see our Rural Healthcare Guide.

Preparing you for the connected future of healthcare

Today, as a healthcare provider, you face evolving demands, including the growth of digital health requirements, data management, EHR optimization challenges and cybersecurity. With the reality of limited budgets, it's important to understand how to effectively evaluate, plan and implement network improvements. Let the healthcare IT solutions experts at Spectrum Enterprise help.

Learn more

1. Mohammad Hasan, "State of IoT 2022: Number of Connected IoT Devices Growing 18% to 14.4 Billion Globally," IoT Analytics, May 18, 2022.
2. "PwC Pulse Survey: Managing Business Risks," PwC, August 18, 2022.

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.

Spectrum ENTERPRISE™