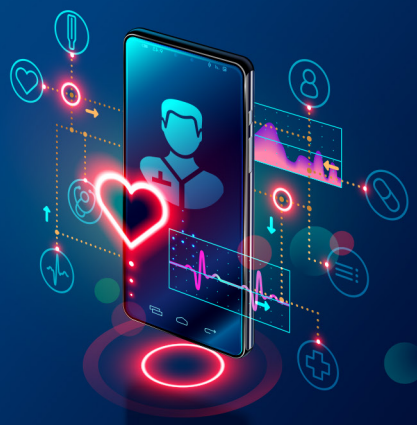
The 3 Pillars of Successful Telehealth



The COVID-19 pandemic has put unprecedented demand on America's healthcare providers. Further complicating the situation, COVID-19 has simultaneously increased the risk of infection for patients and providers alike. This combination of factors makes telehealth services essential to the delivery of safe, high-quality patient care.

To fulfill this need, the offices of Health and Human Services, the Office for Civil Rights, and the Centers for Medicare and Medicaid Services have changed their privacy and payment policies to promote telehealth services. To support these organizations' efforts and to expand access to telehealth services to those who most need it, the Federal Communications Commission (FCC) has also established the COVID-19 Telehealth Program. This $200 million fund will help healthcare providers fund the costs of the technology required to deliver telehealth services effectively and safely. Nonprofit and public healthcare providers alike are eligible to apply for these FCC funds.

In order to help providers make the transition to telehealth as smoothly as possible, we have put together this guide to simplify the process. By selecting the correct three solutions for broadband, video conferencing, and network security, providers can maintain HIPAA compliance, connect with patients, and deliver the same level of care they offer in the office.

Fast, robust connectivity is your patients' lifeline.

To offer quality care, providers need a fast and robust connection to the Internet. While each healthcare organization's precise connectivity requirements will vary based on its particular circumstances, here's why it's important to choose an Internet service provider powered by expert engineering, such as ENA.

As Internet usage has increased and evolved, so have the attacks on Internet service. 2019 saw the evolution of new forms of DDoS attacks and botnets successfully used to disrupt the Internet service for large companies and state governments. An effective ISP will actively scan its network to contain attacks before they disrupt service to keep patients—and their data—safe. An effective ISP will actively monitor and scan its network to detect and contain attacks before they disrupt the service across an entire provider network—thus protecting ongoing services and patient data.

Furthermore, because telehealth services involve patients at their most sensitive moments, it is essential that the connectivity be as robust as possible. An effective ISP will design its network with as much redundancy as possible to ensure connectivity disruption is minimized even in the event of trouble. That means providers can count on their connectivity when patients count on them. And when telehealth services are a patient's only means of accessing life-saving healthcare, the quality of the provider's connectivity is a matter of life and death.

2 Your video-conferencing platform must be as responsive to patients as you are AND comply with their privacy needs.

When patient healthcare and security are on the line, risks are unacceptable. Providers can ensure optimal care by deploying unified communications and video conferencing solutions that are easy to use, cost-effective, and secure. Selecting a platform with a wide selection of security and privacy settings, as well as capabilities for multi-person conferences, makes it easy to coordinate care among multiple providers.

Zoom Video collaboration maintains HIPAA-compliance without sacrificing ease of use. It does so through a host of safety features, including firewall compatibility, medical device integration, 128-bit AES video encryption, and password-protected meetings. With Zoom, gain security without sacrificing accessibility.

3 Hackers are always probing your network for weakness. Always.

Healthcare providers need to assume that hackers are trying to break into their networks at all times. Worse, they need to assume that if hackers do find a way into a network, they will try to steal patient data.

Indeed, according to one report, more than 41 million American patients had their data compromised in 2019 alone, making an increase of nearly 50% from the previous year. With more patient care now delivered online, providers can expect hackers to intensify their efforts.

To foil hackers and protect patient data, healthcare providers must take a holistic approach to security. A key security layer for protecting data is the deployment of a unified threat management system that offers deep visibility into a network. Because ENA's NetShield UTM is designed to do just that, it allows providers to manage applications, ports, protocols, and more in order to meet their specific needs. With such visibility and control, healthcare providers can identify—and address—security weaknesses before hackers do. That keeps patients and their data safe.

Let's work together to bring innovative healthcare solutions to your community

About ENA

ENA delivers transformative connectivity, communication, cloud, cybersecurity, and technology services. Our 99% customer satisfaction rating and world-class net promoter score (NPS) demonstrate our commitment to delivering exceptional customer care. For more information, please visit **www.ena.com**, call **866-615-1101**, or email **info@ena.com**.