VERTIV WHITE PAPER

Telehealth and the Edge of the Network

Infrastructure Considerations for Remote Patient Care

Introduction

The global pandemic had countless direct and indirect effects on the way we live and work. Nowhere is this more apparent than in the healthcare space. While hospitals and frontline workers battled COVID-19 in the trenches and continue to do so, there were other, less obvious actions that are fundamentally changing the healthcare model. Chief among these is the rise of telehealth, a previously simmering patient engagement option that erupted with the pandemic.

The widespread stay-at-home advisories forced the cancellation or postponement of many medical appointments and procedures, and physicians and health systems responded by ramping up what, in most cases, were little-used or non-existent telehealth systems.

Quantifying the Impact of COVID-19 on Telehealth

Before the pandemic, nearly 80% of hospitals in the United States had some level of telehealth service, but only 8% of consumers had ever used such a service[1]. COVID-19 changed everything. Telehealth claim lines increased more than 4,000% nationally from March 2019 to March 2020[2].

It's not an exaggeration to say COVID-19 created a new healthcare delivery model virtually overnight — a model that will endure long after the current pandemic subsides. The World Health Organization designated COVID-19 a "public health emergency of international concern" on Jan. 31, 2020, the fifth such declaration since 2014. There will be other health crises, and as patients become more comfortable with telehealth, any expectation the industry will revert to pre-pandemic practices becomes less and less realistic. In fact, the global telehealth market is expected to grow dramatically, reaching $266.8 billion by 2026 and showing a compound annual growth rate (CAGR) of 23.4% between 2018 and 2026[3].

And why not? Telehealth has the potential to reduce the cost of care, improve access for low-income and rural patients, deliver faster diagnoses and treatment plans, reduce readmission rates, improve patient satisfaction, and increase the frequency and effectiveness of follow-up care. The biggest barrier to pre-pandemic adoption was behavioral inertia. Now due to COVID-19, momentum is building toward a marked transformation.

Understandably, most healthcare providers are struggling to keep pace with this shift. Existing IT systems, infrastructure, and security and privacy protocols already were stretched or outdated due to the proliferation of diversified healthcare systems. Telehealth adds another layer of complexity requiring new IT strategies and investments. Critical decisions are looming for healthcare IT managers and chief information officers (CIOs).

Distributed Healthcare and Telehealth

Long before anyone had heard of COVID-19, the healthcare system underwent another significant evolution to its business model. Distributed healthcare took the hospital-centric approach to healthcare and scattered it, establishing separate, remote facilities for everything from physicians' offices and retail clinics to imaging suites and surgical centers. The objective was to make access to these services easier and less intimidating to patients, improve efficiency and quality of service, and promote accountability across the health system. The results have been mixed on some elements, but the increased access is undeniable. Patient expectations have changed, and for that reason alone decentralized healthcare is here to stay.

That creates some obvious challenges when it comes to telehealth. These distributed locations were established to encourage patients to come to them and to make those visits as easy and enjoyable as possible. They were not designed to facilitate physician-patient video calls and other forms of telehealth. In many cases, these facilities lack the IT systems and infrastructure needed to provide secure, efficient telehealth services.

In short order, these distributed sites have shifted from fairly simple IT needs largely focused on supporting basic data collection and financial transactions to life- and mission-critical patient care hubs requiring robust, sophisticated computing capabilities. Remote imaging centers conduct data-intensive MRIs and CT scans, and high-definition versions of those data files are shared across health networks.

The U.S. government, in response to the pandemic and the urgent need for telehealth services, issued a Notification of Enforcement Discretion[4] that relaxed some HIPAA regulations around the use of platforms such as Zoom, Skype, Apple FaceTime, Facebook Messenger, Google Hangouts and Whatsapp. Still, even if a small office is relying on such platforms for their telehealth efforts, the underlying IT systems must provide adequate network security and reliability.

Keep in mind: These aren't always simple two-way communications. It's not uncommon today to have simultaneous patient calls with multiple physicians at multiple sites. Simply put, telehealth across these distributed health systems is far more complex than anyone could have imagined even two years ago, and the IT systems too often lack the sophistication needed to make it all work.

Telehealth and the Edge of the Network

As healthcare systems have become more distributed, their IT networks have become more reliant on the edge of their networks. Those edge sites often started as fairly simple IT deployments without much consideration of power protection, cooling, or connectivity, and with good reason — computations were at a modest level, and they were not considered mission critical. Downtime was inconvenient, but not crippling.

That has been changing as more and more health services transition to distributed sites, and the surge in telehealth is accelerating that change. As a result, healthcare providers are catching up to a broader trend in the data center ecosystem — increased sophistication of the edge.

The level of sophistication depends on the type of edge site. Using Vertiv's edge archetypes, healthcare IT in the age of COVID-19 and telehealth falls firmly in the Life Critical archetype, meaning IT availability and performance directly impacts human health and safety. That places a premium on the infrastructure supporting those healthcare edge IT systems.

Edge Archetypes

Vertiv studied the spectrum of network edge use cases, focusing on workload requirements and corresponding needs for performance, availability, and security, and identified four main archetypes:

- **Data Intensive** - This includes use cases where the amount of data makes it impractical to transfer over the network directly to the cloud or from the cloud to point-of-use due to data volume, cost, or bandwidth issues. Examples include smart cities, smart factories, smart homes/buildings, high-definition content distribution, high-performance computing, restricted connectivity, virtual reality, and oil and gas digitization.
- **Human-Latency Sensitive** - This archetype includes use cases where services are optimized for human consumption, and it is all about speed. Delayed data delivery negatively impacts a user's technology experience, potentially reducing a retailer's sales and profitability. Use cases include smart retail, augmented reality, website optimization, and natural language processing.
- **Machine-to-Machine Latency Sensitive** - Speed also is the defining characteristic of this archetype, which includes the arbitrage market, smart grid, smart security, real-time analytics, low-latency content distribution, and defense force simulation. Because machines are able to process data much faster than humans, the consequences for slow delivery are high. For example, delays in commodities and stock trading, where prices fluctuate within fractions of a second, may turn potential gains into losses.
- **Life Critical** - This archetype encompasses use cases that directly impact human health and safety. Consequently, low latency and reliability are vital. Use cases include smart transportation, digital health, connected/autonomous cars, autonomous robots, and drones. Autonomous vehicles, for example, must have updated data to operate safely, as is the case with drones that may be used for e-commerce and package delivery.

Edge Requirements for Telehealth

As with traditional healthcare, the focus for the telehealth provider is on providing superior patient care as cost-effectively as possible. Ensuring telehealth services meet patient expectations requires a more robust edge network than we have seen in traditional healthcare models. The priorities for these edge systems are clear:

1. Availability – This refers not just to traditional network uptime considerations, but also uninterrupted connectivity across distributed sites. In a distributed network, connectivity and availability are virtually synonymous.

2. Security – HIPAA laws contain no exceptions for remote healthcare. The security of patient health information is non-negotiable.

3. Scalability – Today's distributed sites lack readily available floor space, so adding capacity and additional equipment must be done wisely and only as needed.

4. Serviceability – In these distributed health systems, there typically are no IT support personnel on site. Designing to minimize service requirements and enable remote monitoring and service is critical.

Note that the focus here is on distributed sites and the edge, understanding that those sites maintain connections to a core data center and often cloud resources that support certain applications. Those facilities are more prepared to support telehealth. The most significant changes — and investments — are needed at the edge.

Availability

In the past, it has not been uncommon to find IT closets in distributed healthcare sites that operated without an uninterruptible power supply (UPS) system. Fortunately, that practice is receding, as it is untenable in today's mission-critical sites supporting telehealth. As the edge of the network has become more important across all sectors, the options for smaller, single-phase UPS systems used to support smaller IT deployments have increased. These are the preferred option in most smaller healthcare locations, although there may be interest in three-phase UPS systems if the load warrants it.

Batteries are an important consideration when choosing a UPS. Valve-regulated lead-acid (VRLA) batteries have been the preferred choice in data centers for decades, but that has started to change. Lithium-ion batteries — variants of which are used in laptops, cellphones and other electronics — have become a popular alternative to VRLA and should be considered strongly in any healthcare facility. Lithium-ion batteries are smaller and lighter than VRLA, and they last longer — all characteristics that play well in smaller distributed healthcare centers and their IT rooms. Accelerated adoption of lithium-ion has brought prices down well past the point of a preferable total cost of ownership.

The other leading variable when it comes to small-space availability is thermal management. Again, this issue has been ignored in many low-capacity healthcare IT rooms, but as demands on IT systems increase and capacity along with them, cooling those systems becomes more of a challenge. More equipment means more heat, and dedicated IT cooling is needed to ensure availability in those spaces.

Security

HIPAA laws codify what healthcare providers have always known — protecting the privacy of patients' health history is no less important than delivering proper care. The decentralization of the healthcare network and now the explosion in telehealth have dramatically multiplied the network endpoints and potential points of access for bad actors. Providers must secure these networks to prevent data breaches. There are a number of tools and appliances available to harden the IT networks in these distributed sites and ensure safe, secure telehealth interactions.

Serial console servers and secure gateways ensure smooth, secure network access while effectively isolating systems to prevent extensive network access from any single point of entry. They enable secure, real-time monitoring, access and control of IT systems, and are a valuable tool for any security-focused edge deployment.

Scalability

The increased use of telehealth resulted in a corresponding increase in capacity demands in these distributed sites, creating an awareness of capacity management that often was lacking in the healthcare space. Of course, healthcare CIOs always reacted to growth or contraction, but in the past, it was more gradual.

The IT systems supporting telehealth require flexibility and scalability to meet that 23% CAGR discussed earlier. Modular solutions provide incremental, packaged IT capacity and infrastructure to meet needs as they arise. These modules can be deployed and configured quickly, meeting urgent demands

Serviceability

A hospital may have a dedicated, on-site IT support team but most distributed sites do not. As these sites become more critical and support urgent telehealth communications, delays in IT support and service are not acceptable. Maintaining availability and connectivity without on-site support requires proactive planning.

The strength of the service organization is one of the most significant differentiators between equipment providers. Without in-house, on-site IT support, having a partner with a large, well-trained service team provides peace of mind that any issues can be addressed quickly and competently.

Embedded intelligence across systems also enables remote monitoring and maintenance, so problems can be detected quickly and often addressed without a service call. Or, if a service visit is necessary, the technician arrives with an understanding of the problem and the parts needed to make the fix. Not all IT equipment is equipped with that kind of intelligence, so choose wisely when provisioning for those edge locations.

Conclusion

Widespread adoption of telehealth across distributed health systems that rely on edge networks presents new challenges for today's hospitals and healthcare providers — specifically increased demand for low-latency computing and security. Decision-makers must deploy their IT resources with that in mind while still managing the needs for sudden capacity increases and always-on availability. There are some edge best practices outlined in this paper that may be used as a guide to address these unique challenges.

Visit Vertiv online to learn more about healthcare network infrastructure and solutions to support telehealth, or to find the representative nearest you.

[1] https://static.americanwell.com/app/uploads/2019/07/American-Well-Telehealth-Index-2019-Consumer-Survey-eBook2.pdf
[2] https://www.healthcarefinancenews.com/news/telehealth-claim-lines-increased-more-4000-past-year
[3] https://www.fortunebusinessinsights.com/industry-reports/telemedicine-market-101067
[4] https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf

Vertiv.com | Vertiv Headquarters, 1050 Dearborn Drive, Columbus, OH, 43085, USA