caregility
Connecting Care Everywhere

Virtual Care Network Security Without Clinical Disruption

Tele-nursing, tele-sitting, and tele-consults represent just a few of the virtual care programs gaining prominence in hospitals. As hybrid care models that blend remote and in-person caregivers expand, enterprise telehealth is paving the way for virtual engagement at every patient's bedside.

Under this new paradigm, healthcare IT teams are understandably looking to drive security standards across rapidly expanding virtual workflows. The challenge is that many corporate IT standards around network security and performance can disrupt patient care in always-on virtual environments where devices must be available 24/7.

Common Network Security Standards that Negatively Impact Virtual Care

- ***Login expirations***
  It's common for cybersecurity teams to force users to log out at certain intervals. That means tele-sitters may need to log back in multiple times during a shift, interrupting patient observation.

- ***Device timeouts***
  To keep unused devices from overloading the network, sometimes idle systems that are on for a certain number of hours are automatically disconnected. If you're in the middle of monitoring a patient and that connection drops, that creates a safety risk for that patient.

- ***Firewall port restrictions***
  Firewall updates frequently disconnect virtual care applications. If you're a virtual sitter watching a patient, your system disconnects, and you can't call back in, the time it takes to reestablish access to a high-risk patient can feel like an eternity.

- ***DHCP registration requirements***
  When managing IP addresses, enterprises often reset assigned addresses, sometimes as often as every 30 minutes. This can cause disconnects. If multiple systems are trying to renew their IP lease at once, it can cause congestion. If you're a doctor trying to call into a patient room that's still in queue to get an IP address, that call will not connect.

- ***Wi-Fi over-subscription***
  You can have excellent coverage when you evaluate your Wi-Fi heat map, but it's really about network congestion. How many devices are connected to your access points transmitting data? That can impact connectivity and disrupt care during periods of high traffic.

- ***Bandwidth restrictions***
  Most networks are designed for data applications, not two-way video. This leads to bandwidth strain during peak usage times when concurrent session rates are high.

Virtual Care Network and Security Best Practices Checklist

It's essential that your hospital clinical and IT teams connect early on, collaborate, and are willing to compromise to support network and security in a way that does not disrupt virtual patient care.

Follow these best practices to ensure your network is optimized for bidirectional virtual engagement:

- ☐ Compromise on staff login expirations by having automatic logouts coincide with shift changes.
- ☐ Avoid automatic disconnection of devices used in hybrid care models.
- ☐ Use static IP addresses for virtual care resources if you can. If not, at least have a reserve of IP addresses designated to virtual care support and set the IP lease to last a full shift.
- ☐ Measure the experience of your Wi-Fi-connected devices and calculate how many devices are within a wireless access point. How much are they being used? Can they be hijacked?
- ☐ Calculate your peak bandwidth. Look at your fleet of devices, review your network capacity, and estimate the number of concurrent connections you can comfortably do. Then design your network to what that peak bandwidth threshold would be.
- ☐ Hardwire virtual care devices whenever possible to reduce the potential for connectivity interruption.
- ☐ Empower patients to connect with their family, care team, and interpreters but consider that impact on call volumes when multiplied across the entire hospital. Factor this into peak utilization because what you don't want is to have a lot of patients socializing with their families while your doctors can't access the tele-ICU because of bandwidth limitations.
- ☐ Remember that network conditions at clinician workstations will also impact virtual session performance. Ensure nurses and physicians are allocated enough bandwidth to support multiple concurrent connections.
- ☐ Isolate high-intensity connections like tele-ICU traffic to a VLAN virtual network where their bandwidth is protected. Leave concurrency available for high-profile locations and only allow so many ad-hoc calls to happen simultaneously to ensure high-priority sessions are maintained.
- ☐ Isolate video traffic in a VLAN if possible or create a wireless environment that's only for virtual communications. This is going to become particularly important as health systems deploy video systems in every patient room to support enterprise-wide virtual nursing and patient engagement.
- ☐ Invest in tools that help you monitor and assess your network to quickly pinpoint and proactively address issues.
- ☐ Get feedback from your clinical team. The easier you make virtual care to use, the less it becomes technology and the more it becomes a tool for clinicians to provide better care.
- ☐ Bring the cybersecurity team, the network team, and technology partners in early on. Talk through the impact of virtual workflows on the clinician and patient experience. Understand what you need to do to meet cybersecurity and network demands within that environment.