

Case Study

CBTS transforms a healthcare provider's wireless network, expanding access to mobile devices, hardening security, and streamlining patient treatment

Client

Regional healthcare provider

A hospital system based in a U.S. city with a population over 500,000 uses wireless technology to connect medical professionals with each other and their patients. CBTS implemented a comprehensive upgrade of the healthcare provider's LAN and WLAN systems.

Challenges	CBTS solutions	Results
<ul style="list-style-type: none"> • Wi-Fi network must be able to connect up to 30 devices per patient room, but the organization's aging network could not handle the demand. • Dead spots in WLAN coverage dropped connections to wireless devices, slowing operations and threatening patient care. • Poor security in many wireless medical devices poses an intrusion risk. 	<ul style="list-style-type: none"> • CBTS audited the entire WLAN environment to identify devices and map out opportunities to improve services. • Built out a new LAN and WLAN architecture • Aruba Networks and HPE Smart Rate technologies deliver 2.5-gigabit WLAN connections, fulfilling capacity requirements and eliminating dead spots. • Device profiling elevates security. • Meets all compliance guidelines. 	<ul style="list-style-type: none"> • The healthcare organization's high-capacity WLAN ready for advanced technologies like the Internet of Things. • Healthcare providers no longer experience dropped connections, streamlining operations and reducing risks to patient care. • Security protocols prevent hackers from breaking into unsecured devices. • Network complexity and cabling costs were reduced.

Challenges

The healthcare organization needs to upgrade its wireless network so that it can handle up to 30 connected devices per patient room. The company's aging wireless network could not handle those demands.

The organization's legacy WLAN had critical dead-spot issues. Doctors and nurses carrying mobile devices from one floor to another or to nearby buildings would lose their WLAN connection, forcing a reconnect that took five to 15 minutes. That delay made care delivery less efficient and threatened to impact patient health.

Some medical devices were inherently insecure because they lacked a built-in operating system. These vulnerabilities needed to be repaired.

Each WLAN access point required two cables to deliver a 2-gigabit connection, increasing complexity and cost.

CBTS solutions

CBTS partnered with Aruba Networks, an HPE company widely considered the industry's top enterprise wireless technology provider. CBTS designed and implemented a full turnkey solution that:

- Audited the entire WLAN environment to identify devices and map out opportunities to improve services.
- Built out a new LAN and WLAN architecture, using HPE Smart Rate technology to deliver 2.5-gigabit interfaces to each wireless access point
- Created device profiles for each smartphone, tablet, and multiple varieties of mobile medical devices. Rules for each of these devices controlled access and maintained security.
- Fulfilled capacity and bandwidth demands while cutting cabling requirements in half.
- Used device segregation and isolation to tighten network security.
- Complied with the PCI payment standard and other regulatory guidelines.
- Used Aruba Clear Pass technology to create a common configuration for network switches.

Results

The new Wi-Fi system supports thousands of connected devices, clearing a path to advanced technologies like the Internet of Things.

Doctors, nurses, and other medical professionals can travel from floor to floor and to multiple nearby buildings without losing their wireless connection. Operations are more efficient, and there's far less risk of a lost connection endangering patient care.

Security protocols prevent hackers from breaking into medical devices that lack operating systems and security controls. Guest traffic is isolated from internal patient traffic, and each device has sophisticated credentialing that prevents unauthorized access.

Network complexity and cabling costs are reduced. The number of wireless networks was reduced from dozens to just three.

Connections are compliant with regulatory standards such as PII, PHI, and PCI.