

This is the third Insight in our three-part series outlining challenges health systems face when choosing smart devices, upgrading security, and evaluating network reliability to support clinical communication and collaboration technologies.

### Facility Design

Anyone working in a healthcare facility knows there are “dead zones” where there is no connectivity for smart devices. The age of the building and type of building materials - like metal lath and plaster - can create issues with connectivity. Fire codes often do not allow Wi-Fi access point installations, and connectivity can be interrupted by fire-safe steel doors. Dead zones often occur in elevators or in shielded areas such as MRI and radiology departments. Employees have learned to live with these dead zones, especially if the devices and applications they are using don’t necessitate a more robust networking system.

Adding a clinical communication and collaboration platform not only requires more from the devices being used, but from wireless network systems, as well. This is particularly critical when using voice over Wi-Fi, because of the need for clear and fast communication as users walk and talk throughout the facility during their shifts.

### Network Connectivity

An upgrade to a smart device requires better connectivity, which can increase dramatically depending on the number of devices and how many new applications are running. Will devices be supporting voice and how is the quality? Is the network environment set up to express forward voice and video services over others, and are your firewalls correctly set up to accommodate interactions between applications? Express Forwarding (EF) is a Quality of Service (QoS) mechanism in a network environment that assures a good end-user experience in your environment by prioritizing real-time communications over general network traffic.

Some of the biggest items that are commonly missed are the number of Wi-Fi access points as well as the layout of those points. Both should be reviewed during a full network assessment, and if necessary, a new layout plan should be completed.

### Network Load

One of the biggest pitfalls health systems face is believing that the current network will continue to work as well when new devices are added to the system. But imagine adding 1,000 new mobile devices to the network, on a communication platform that includes messaging, voice, system alerts and scheduling - the network load and connectivity can go through the roof. The best times for health systems to upgrade and optimize their networks is when they are upgrading and adding new devices.

During the full network assessment, health systems need to determine hardware, software and firmware versions, and their compatibility with the network: Will the newest devices be supported by the existing infrastructure? Complexity increases as you add hospital-provided devices that nurses and clinical staff use, versus bring your own device (BYOD) which providers most often use.

When health systems upgrade their communications systems, they need to address the networking challenges of implementing a clinical communication platform, staff workflows, and the assortment of devices being used. Ensuring your network is ready will increase user satisfaction with the new system and lead to improved communications and adoption among staff.



Read the other two Insights in this series:  
[Smart Devices in a 24/7/365 Work Environment](#)  
[Hitting a Moving Target: Securing Healthcare Devices](#)