THE SMART WAY FOR HEALTHCARE ORGANIZATIONS TO GO MOBILE

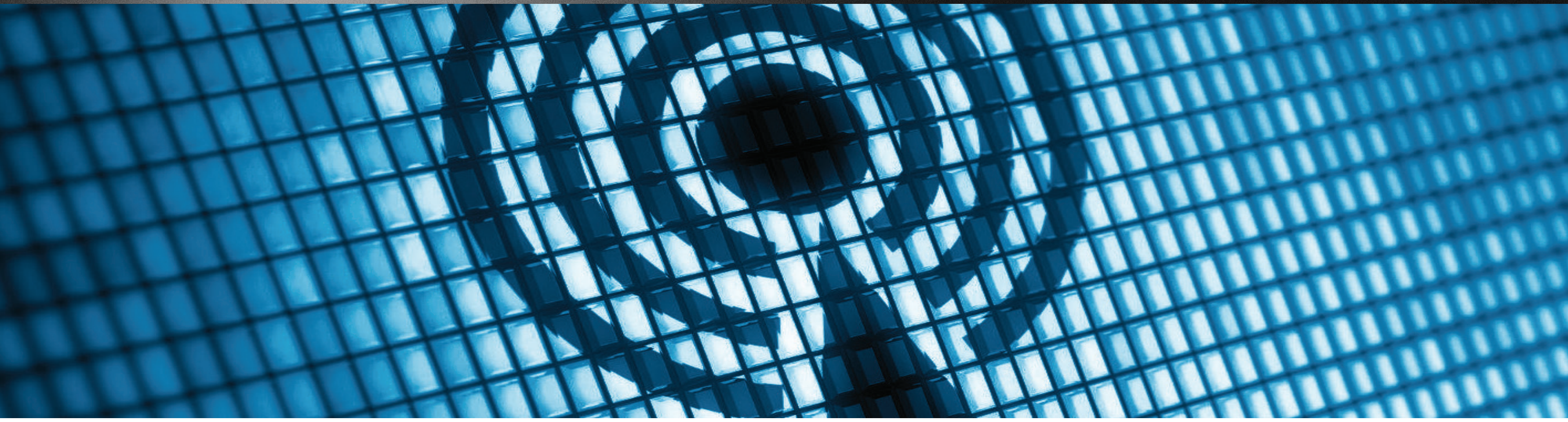
INTRODUCTION

On January 1, 2014, a key provision of the American Recovery and Reinvestment Act of 2009 went into effect, requiring healthcare providers across the country to adopt and demonstrate "meaningful use" of electronic medical records (EMR) in order to maintain their existing Medicaid and Medicare reimbursement levels. Providers who make the minimum IT investment required to digitize their data soon discover that their daily routines and workflows have become seriously disrupted. With records now stored on servers instead of in filing cabinets, reliance on computers and networks take on a whole new level of importance, too. Many healthcare providers are finding that adopting wireless mobile solutions are a must-have to more accessible and updated EMRs and streamline workflow processes.

The decision to go mobile, however, brings new challenges, ranging from selecting the appropriate form factor to ensuring mobile devices and wireless communication are secured from unauthorized users. Making the decision even more difficult is the number of mobile devices flooding the market. According to Gartner, tablet vendors sold more than 195 million tablets in 2013 with various operating systems, up 68% from the previous year. Consumer electronics manufacturers have done a great job getting the message out that people's lives can be happier and more productive with the latest lightweight tablet and ubiquitous access to the Internet. In the commercials, users seamlessly transition from watching a movie on their tablet device to their television; pictures, videos, and other content is shared easily among devices after two similar devices come in contact with one another; and a high definition streaming experience is achieved everywhere.

In a healthcare environment, where organizations desire many of the same productivity-enhancing benefits as their consumer counterparts, consumer grade tablets are making a foray into doctor's offices, hospitals, and other specialty care facilities. What the consumer tablet commercials fail to warn us about, however, is that healthcare organizations have several requirements that consumer devices — and consumer wireless networks — weren't designed to address. What's more is the fact that clinicians and other healthcare workers need fast, reliable access to patient records and other clinical data in order to realize productivity gains over traditional practices. And, patient information needs to be properly protected in order to comply with HIPAA and Joint Commission (formerly JCAHO) requirements.

In this whitepaper, we'll explore the critical advantages for choosing purpose-built mobile devices and business-grade wireless networks in a healthcare environment. We'll also highlight best practices for selecting mobile devices and building wireless infrastructures.



BUSINESS-CLASS VS. CONSUMER-GRADE WIRELESS NETWORKS

Today's tech-savvy consumers can set up wireless networks in their homes in three easy steps that take less than three minutes to complete:

Step 1 – *Remove the wireless router from the box and connect an Ethernet cable from the router to a cable or DSL modem.*

Step 2 – *Plug in the wireless router and turn it on.*

Step 3 – *Using a Wi-Fi-enabled mobile device type in the wireless router's 20-digit alpha-numeric code, found on the bottom of the wireless router.*

Voila, you now have wireless.

Unfortunately, some healthcare practices apply the same plug-and-play mentality when deploying wireless networks in the work environment. Hospital and clinical care wireless networks have two major differences from most other types of wireless enterprise networks. First, they are considered mission critical, meaning that most of the business conducted over them can radically alter the quality of life and the delivery of critical patient care. And second, they need to be highly secure; there is a large amount of information that is transmitted over these networks that is required by many regulatory agencies and the Federal Government to be kept highly confidential.

Clinicians have grown used to the reliability of wired networks. However, "going mobile" and accessing data over a wireless network deployed in the three-step manner outlined above, will produce less-than-reliable user experience. For example, during high traffic periods when multiple healthcare workers are accessing the network simultaneously, some users will be dropped from the network while others will experience the equally irritating effect of the "hourglass" on the screen icon as the mobile device attempts to send and receive data using the sliver of bandwidth available on the network. In an environment where data is used to make important decisions, problems such as data bottlenecks, dropped connections, and mobile device freeze-ups are unacceptable.

Another factor that physicians and other healthcare IT decision makers need to consider before deploying wireless networks is the potential negative impact on their wired networks. In addition to creating a poor wireless networking experience for mobile computer users, the workstations tethered to the wired network will likely experience similar problems due to the two networks vying for the same bandwidth.

If a poor user experience wasn't bad enough, a consumer Wi-Fi network falls short in the area of security too. Despite the fact that a wireless router may use password protection, there are several other factors that must be taken into consideration before a router can be deemed

"secure." For example, the SANS Institute, a private U.S. company that specializes in Internet security training, created a whitepaper titled: "Securing Wireless Networks for HIPAA Compliance."
According to the article, there are five standards healthcare providers need to follow to ensure their wireless networks are encrypted, including:

1. **Access control** — just as the name implies, controlling who is granted access to the organization's resources.

2. **Auditing** — maintaining logs of who accessed a given resource at what time and where so that in the event of a security compromise there will be an audit trail.

3. **Integrity** — includes making sure that PHI (protected healthcare information) is not modified in any way by an unauthorized user during transmission or storage.

4. **Person authentication** — authenticating that the person the computer says they are is really the correct person accessing the wireless network.

5. **Transmission security** — ensuring that wireless network transmissions are kept private.

In the next section, we'll explore best practices for deploying a business-class wireless network that addresses each of these criteria.

3 TIPS FOR DEPLOYING A HIPAA-COMPLIANT WI-FI NETWORK

Unlike the home or traditional small business environment, deploying a wireless network in a healthcare setting is much more complex. For example, it's not unusual in a hospital setting to have dozens of different devices and literally hundreds of applications being used at any one time. Plus, certain patient care areas within a hospital have their own special needs — all of which require careful planning and the perspective of multiple stakeholders.
Following are three tips to keep in mind before deploying a wireless network in a hospital environment:

THE PHYSICAL BUILDING

Even though this is the most obvious area of the three, it's also the most challenging. When conducting a wireless survey, it's important to call out wireless inhibitors within the facility, which may include materials such as brick, block, and wireless mesh. In addition to conducting a general site survey, extra attention should be given to specialty care areas within a medical care facility such as radiology, oncology, Bio medical areas, operating rooms, autoclaves, and labs which use equipment that can be very disruptive to some Wi-Fi signals.

In addition to obstacles that obstruct RF signals within the building, wireless bleed-through needs to be accounted for. For example, the wireless signal from the second floor may inadvertently extend to the third floor. One problem this could create is that when a user on the third floor connects to the weaker signal (inadvertently or intentionally), the connection may drop after a short period, resulting in a disruption for the user on the third floor and potentially for users on the second floor. Another reason this issue needs to be resolved upfront is that it could compromise location-based access control policies, which are an important part of the hospital's IT security and compliance requirements.

END USERS

Without proper forethought and planning, one or more groups of key stakeholders will most likely be overlooked during the wireless infrastructure planning process. In a hospital setting, for example, in addition to the doctors and nurses that regularly work on a specific floor and in a particular area of a hospital, other clinical staff such as visiting physicians, specialty care, pharmacy, and hospice should be accounted for. Additionally, non-clinical staff such as security personnel, dietary staff, IT, administration, volunteers, and facilities personnel may need access to the network to better perform their jobs. Proper bandwidth and security measures need to be put into place for these workers.

And finally, patients and guests are an important part of the hospital ecosystem that should be accounted for too.

DETERMINE ACCESS PRIORITIES

With careful wireless network planning, healthcare providers can gain a better sense of how much bandwidth is necessary to support their mobile user ecosystem.

However, due to the widely varying load on the network — both in terms of the number of physical users accessing the network at any given time plus the types of applications being accessed, it's impossible to build a perfectly elastic network that never experiences bottlenecks. With that in mind, it's important to add quality of service (QoS) capabilities to the wireless network design. Doing so will ensure that during heavy network use, the clinicians, whose use of the network is mission critical and directly affects patient care, can perform their job duties without network- and application-related delays or interruptions.

3 REASONS PURPOSE-BUILT MOBILE DEVICES ARE ESSENTIAL

In addition to designing the proper wireless network, choosing the right mobile device is a critical part of the process that must be handled with care. As mentioned earlier, consumer devices are making a foray into the healthcare environment. After all, they're less expensive than purpose-built devices, and users are often already familiar with their interfaces, so there's a shorter learning curve — what's not to like, right? Before you make that call for your healthcare organization, consider the following three advantages of a purpose-built mobile device.

TCO (TOTAL COST OF OWNERSHIP)

Out of the myriad of benefits consumer-grade manufacturers highlight in their commercials, TCO (compared to a rugged device) is never one of them, and for good reason. According to VDC Research, rugged device TCO is considerably lower in comparison to non-rugged device TCO. In fact, the report notes that "popular" (i.e. non-rugged) tablets have a failure rate that exceeds 15%, which is more than five times as often as rugged tablets. Some of the most common reasons for device failure are due to: dropped devices, software-related issues, water/liquid exposure, and unauthorized changes to devices.

In addition to the hard costs associated with repairing or replacing devices, healthcare organizations need to consider the soft costs associated with downtime, which has a negative direct impact on worker productivity and patient care. These were concerns Graphium Health took into consideration when it rolled out its first product offering, AnesthesiaEMR.com, a web-based application that digitizes the existing intraoperative anesthesia form. This application allows users to document via a tablet PC, effectively connecting the anesthesiologist to the cloud. According to Jeffrey R. Zavaleta, M.D., private practice pediatric anesthesiologist and chief medical officer of Graphium Health, “Compared to what’s out on the market, the Motion Tablet PCs have three distinct advantages: first the durability is unsurpassed, and common disinfectant wipes easily cleansed contaminated units; second, the stylus input was a must for our ‘digital pen and paper’ solution; finally the Windows operating system allows our IT department to easily disk image and support the hardware.”

COMPATIBILITY WITH ENTERPRISE SOFTWARE

The VDC Research report mentioned earlier goes on to site iOS and Android-based consumer mobile devices’ lack of accessories to support mobile workflows and their inability to support current systems as additional reasons businesses should consider Windows-based rugged alternatives. A more recent research study, commissioned by Intel, delved into the limitations and challenges Android and iOS devices create in a business environment. The report summarized the research, stating: “Windows 8 tablets provide a PC experience, which for many workers is essential to maintaining productivity. With Windows 8, users can run familiar desktop applications, maintaining productivity without having to find new ways to carry out their tasks. They can read, edit, and print their emails and Office documents—tasks that can be a challenge on other tablets.”

Choosing a tablet with a Windows 7/8 operating system was a key deciding factor in Graphium Health’s decision making process, mentioned by Dr. Zavaleta above. It was also an important part of East Jefferson General Hospital’s selection process, when the hospital implemented a mobile point of care solution that it integrated with its Cerner EHR as well as other documentation tools such as cameras and bar code scanners. The results of the hospital’s rugged mobile solution included drastically reduced hospital-acquired pressure ulcers, which made a significant improvement in the hospital’s quality of care.

SECURITY

Security is a top concern in a healthcare environment, where patient data breaches can lead to stiff HIPAA fines, in addition to an organization’s loss of reputation. Healthcare organizations that opt to use Android and iOS devices limit themselves to the security and remote management applications supported by those mobile operating systems. Even though these devices may include their own personal security features that allow an individual user to remotely lock or wipe a lost or stolen device, these features aren’t easily extended to IT administrators or IT service providers who may need access to the devices to ensure software updates and patches are being performed regularly. Windows based rugged devices, on the other hand, are purpose built for enterprise environments such as hospitals, and they are designed to support mobile workflows as well as IT security initiatives.

CONCLUSION

In a healthcare environment where patient care needs, improved productivity, and HIPAA compliance must all be taken into consideration with every decision, using consumer devices and consumer-grade wireless networks can be disastrous. Selecting a business-class wireless network and deploying purpose-built mobile devices, on the other hand, is a necessary combination to improving patient care delivery while at the same time maintaining security and increasing retained revenue for the entire business. The additional efforts invested up front in planning and selecting business-grade wireless networks and purpose-built mobile devices means that in the long run the business saves money and has a much higher level of end user and customer satisfaction.