ENGINEERING THE WIRELESS HOSPITAL

Implementing a wireless network in a hospital allows physicians to use state-of-the-art equipment. But there are security, infrastructure and connectivity obstacles to overcome.

COVERAGE IS EVERYTHING

Successful outcomes for wireless networks depend on a correct diagnosis of needs, from access points to VLANs to a real-time location system. **BY STAN GIBSON**

IN JUST A few years, the hospital Wi-Fi network has gone from a nice-to-have add-on to an indispensable IT infrastructure workhorse, carrying far more traffic—and more kinds of traffic—than was once ever imagined. If you're planning a hospital Wi-Fi network today, you have to design it at industrial strength—and then some—or risk a costly retrofit later.

"By the nature of the business, wireless becomes your primary network. Your nurses and doctors are moving around. And tracking devices via RFID will be a huge part of a hospital operation," said Jack Santos, an analyst at research firm Gartner Inc. and former CIO at Catholic Medical Center in Manchester, N.H.

A Wi-Fi network must not only enable guest and patient Internet access, but it must also securely transport electronic health records (EHRs) to and from mobile workstations, Voice over Internet Protocol calls, foreign-language translation services, basic images and, as Santos said, radio frequency identification (RFID)-based real-time location systems (RTLS). It's a tall order.

START AT THE BEGINNING

Any wireless hospital network must begin with a thorough site assessment—and hospitals are sites like no others. Experience has shown that the Wi-Fi network design rules that apply to typical office buildings must

be thrown out the window when planning for a hospital network.

"The biggest issue at first is doing proper surveys. You need to find out where the interference is and on what channels, and build your network from there," said Tom Cotter, enterprise network advisory specialist at Memorial Sloan-Kettering Cancer Center in New York.

YOU CAN'T HAVE TOO MANY WIRELESS ACCESS POINTS. HOSPITALS TYPICALLY REQUIRE DOUBLE, EVEN TRIPLE, THE NUMBER OF ACCESS POINTS THAT ARE TYPICAL OF OTHER INSTALLATIONS.

Zac Bujnoch, an analyst at research firm Frost & Sullivan in San Antonio, noted that hospitals were never designed with wireless networks in mind. Convoluted floor layouts of buildings that may be a century or more old are just the beginning of the problem. Moreover, hospitals are replete with Wi-Fi signal-blocking stainless steel equipment and medical devices that may emit radio frequency interference. Experience has shown IT managers need to allow plenty of time—weeks or months, depending on the size of the facility—and to expect the unexpected.

For Cotter, home Wi-Fi networks in the Upper East Side presented problems. "We have several apartment buildings right across the street. A few years ago, everyone was buying [Wi-Fi equipment] and transmitting at maximum strength. We saw some interference issues, so we had to adjust the power levels and adjust coverage," said Cotter.

Santos experienced interference issues of a different sort. "When we deployed a wireless network in the emergency room, in one corner—and it was an important spot—we had a hard time keeping signals alive. It was because the automatic door mechanism interfered with the signal for the wireless network," he said.

A THOUSAND POINTS OF ACCESS

You can't have too many access points. Hospitals typically require double, even triple, the number of access points that are typical of other installations.

Four years ago, The Ohio State University Medical Center (OSU) began a major wired and wireless network upgrade for a number of hospital and academic buildings encompassing 5 million square feet. After a year of planning, OSU

launched blanket wireless coverage.

"We did an extremely dense implementation. Cisco recommends 3,000 square feet per access point. We did one per 1,000 square feet—and more, in some places—based on the anticipated density of wireless devices," said Chad Neal, director of technology at Columbus-based OSU.

"We covered all clinical areas with the same coverage. We also have coverage in tunnels, where we have robotic carts that handle trash, dishes and linen. We worked very closely to engineer the wireless specs of 'how many access points' and signal strength. We wanted overlapping 'pancakes' of coverage," Neal explained.

SECURITY, TRAFFIC CONTROL, RTLS

Because hospital Wi-Fi networks are carrying patient medical data, IT pros must ensure that the traffic is encrypted, as mandated by the Health Insurance Portability and Accountability Act (HIPAA). Today, that means implementing Wi-Fi Protected Access (WPA2) encryption. WPA2 has superseded Wired Equivalent Privacy (WEP) encryption, which can be readily broken by knowledgeable hackers.

In addition to WPA2, hospitals often implement intrusion detection systems from providers such as AirMagnet (part of Fluke Corp.), AirDefense (from Motorola Inc.) and AirTight Networks Inc. The companies have all developed extensive reporting mechanisms that conform to HIPAA requirements.

> "WE WORKED VERY CLOSELY TO ENGINEER THE WIRELESS SPECS OF 'HOW MANY ACCESS POINTS' AND SIGNAL STRENGTH. WE WANTED OVERLAPPING 'PANCAKES' OF COVERAGE."
>
> —CHAD NEAL
> director of technology, The Ohio State University Medical Center

Because wireless hospital networks are asked to carry such a wide variety of traffic, distinct travel lanes must be provided for each type of traffic, whether it be guest and patient access, medical records and basic images, medical equipment information or RTLS data. Generally, traffic is segregated and assigned to any of several virtual private networks across several different Wi-Fi channels. For example, because Wi-Fi chips are now built into medical equipment such as infusion pumps, those clinical systems are best kept

on a separate channel or virtual LAN (VLAN), Santos noted. "You don't want that to interfere with the data network," he advised.

While extremely high-resolution medical images can't be carried effectively over today's Wi-Fi networks, basic images at lower resolution are often being sent with medical records, which should be on their own separate VLAN or channel. Often, these records and images show up at patients' bedsides on mobile PCs known as COWs (Computers on Wheels) or WOWs (Workstations on Wheels)—medical workstations that can be moved from one bedside to the next and require reliable Wi-Fi access wherever they may happen to be.

Many institutions are also implementing RTLS from any of a number of vendors, including Ekahau Inc. and AeroScout Inc., in order to track expensive equipment such as WOWs, COWs, infusion pumps, X-ray machines and monitoring devices. Taking RTLS a step further, Ekahau recently announced a partnership with Polycom Inc. to enable location tracking on Polycom's SpectraLink 8000 Series Wi-Fi handsets. This will let nurses and doctors reach one another by phone and understand their relative locations.

Any RTLS implementation must assume a steady increase in the number of devices to be tracked. Memorial Sloan-Kettering is implementing an AeroScout system that now tracks 8,000 tagged devices but will cover 12,000 tagged devices next year, according to Cotter.

MANY INSTITUTIONS ARE ALSO IMPLEMENTING RTLS TO TRACK EXPENSIVE EQUIPMENT SUCH AS WOWS, COWS, INFUSION PUMPS, X-RAY MACHINES AND MONITORING DEVICES.

Finally, despite the increasing reliance on Wi-Fi networks, no hospital can do without a high-bandwidth wired network. High-resolution medical images demand it, and the wired LAN provides essential redundancy for the Wi-Fi network. ■

Stan Gibson is a contributing writer to SearchHealthIT.com. Write to him at editor@searchhealthit.com.

Aerohive™

SPIDERS.

PUBLIC SPEAKING.

EXPLAINING WHY YOU NEED $20,000 FOR CONTROLLERS TO SUPPORT ONE MORE THIN AP.

SOME FEARS CAN'T BE EXPLAINED. OTHERS ARE PERFECTLY REASONABLE.

Each time you add an access point in a controller-based WLAN environment, you can become subject to the "controller tax" – that extra charge you didn't factor into adding more APs for coverage or mission-critical apps like voice. And one fateful day you'll add one too many APs and you'll have to foot the bill for a whole new controller – two, if you want redundancy. Kind of makes you nervous just thinking about it, really.

WANT A BETTER WAY TO BUILD A WIRELESS NETWORK? ELIMINATE THE CONTROLLER.

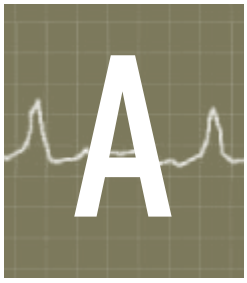
Aerohive's controller-less WLAN architecture provides an innovative alternative to costly and complex controller-based solutions. Aerohive access points organize themselves into groups, or "hives," that cooperate to share information, enabling functions like fast layer 2/layer 3 roaming, coordinated RF management, security, and mesh networking, all without the botlenecks posed by controllers. There is no need to add expensive controllers at every location, because the APs share the information they need. There is no need to engage in controller capacity planning, because you can simply add APs when and where they're needed. So you not only save money, but your WLAN is ready for mission-critical apps like voice-over-WLAN. No controller means you have total control. And that means you have nothing to fear.

Learn more about the economic benefits of Aerohive's unique approach. Download the whitepaper at **www.aerohive.com/economics.**

W W W . A E R O H I V E . C O M

RUNNING THE NETWORK

Wireless networks can do more than track equipment and field phone calls. When adding wireless-enabled devices, though, there can be too much of a good thing. **BY STAN GIBSON**



T SEATTLE-BASED Swedish Medical Center, IT Director Steve Horsley is gathering his share of WOWs thanks to his "Easy Button." When pressed, the Easy Button alerts IT via a radio frequency identification (RFID)-enabled real-time location system (RTLS) and pinpoints where an IT staffer can pick up a stray Workstation on Wheels (WOW).

"In a wired world, doctors and nurses are much more diligent about calling the service desk. With a mobile device, they might shove it in the corner and grab another one until there are none left," Horsley said.

As hospital Wi-Fi networks take on large quantities of diverse traffic, IT pros are discovering best practices such as the Easy Button for getting the most out of their wireless networks.

CURING SPOTTY COVERAGE

As the previous chapter indicated, your wireless network implementation should have been preceded by a thorough site survey to determine the best locations for wireless access points. Once your network is up and running, your work is not done, however. Wi-Fi signal coverage continues to be the highest priority and biggest worry.

"Network management and monitoring are really key. You have to watch carefully for any drops. That's the death knell for a clinician," said

Jack Santos, a Gartner Inc. analyst and former CIO at Catholic Medical Center in Manchester, N.H.

Curtis Larsen, senior wireless engineer at University of Utah Health Care in Salt Lake City, reported having issues with rogue access points in clinical areas. Often, he said, it's because users are trying to accomplish something on their own.

In one instance, an IT manager was trying to provide wireless access to a wired subnetwork. "He decided to plug in an access point," Larsen explained. "So we sat down and discussed his needs and found out we could do the same thing over the central wireless solution, allowing access to those who needed it based on their identity."

Although an initial test might find a clear Wi-Fi signal, new equipment that might cause interference is brought into hospitals all the time. Tom Cotter, enterprise network advisory specialist at Memorial Sloan-Kettering Cancer Center in New York, said he contacts vendors of wireless hospital equipment in advance of any network upgrades to make sure the equipment has been certified not to interfere.

Larsen, meanwhile, is deploying Cisco 3500 Series access points. These include a spectrum analysis feature, through which the access points push alerts to a monitoring and management tool whenever interference is detected, he said.

Installing access points is made easier with open communication among hospital staff members. For example, Larsen said it pays to coordinate with building security to make sure surveillance cameras don't interfere with wireless devices.

In addition to tracking WOWs, Computers on Wheels and a plethora of diverse medical devices, many hospitals are looking ahead to the use of their RTLS infrastructure to track patients using RFID-enabled wristbands. Patients with Alzheimer's disease in particular are thought to be good candidates for future RTLS deployments. Horsley said he's considering such an implementation at Swedish Medical—but over a separate infrared network, not the hospital's 802.11 Wi-Fi network, to avoid interfering with other systems.

Since most people inside a hospital—doctors, nurses, patients and visitors—have cell phones, and since cellular coverage inside a multistory hospital may be spotty, enabling cellular phones to send and receive calls over the Wi-Fi network is becoming a priority for many hospital CIOs. "Many cell phones have Wi-Fi capabilities. And many carriers can take calls that get routed to them from a Wi-Fi network," noted Chad Neal, director of technology at The Ohio State University Medical Center in Columbus.

WI-FI UPGRADES TO CONSIDER

As equipment based on the 802.11n Wi-Fi standard comes onto the market, hospitals are facing equipment upgrades from current 802.11a, b and g implementations.

The 802.11n standard implements multiple-input, multiple-output technology, or the ability to use two antennae for both sending and receiving. The effect is to increase available network bandwidth.

Compatibility is not a major concern, but engineering a smooth upgrade still takes planning and testing. Horsley was faced with purchasing 802.11 a, b and g access points that could be upgraded to the 802.11n standard, or purchasing nonupgradeable units and simply replacing them with new 802.11n gear. He chose the latter course, since the savings on the upgradeable units were negligible and required approximately the same labor for installation and testing.

KNOWING WHEN TO SAY WHEN

Tablet devices, once thought to be an attractive solution for doctors and nurses, remain rare at many hospitals. That may change with devices such as Apple's iPad and Cisco's Cius. Hospital IT pros are taking note. "The doctors are very excited about it. People who use the iPhone and iPod touch are excited" about the iPad, Neal said.

However, he is on guard. "With the iPad, there is a lot of buzz, but it's very challenging for us to identify the business value," Neal said, adding that, ultimately, "it's not an enterprise-friendly device. It's hard to manage."

That points to the biggest challenge for IT pros as hospital Wi-Fi networks take on increased traffic from many different devices—just saying no. "Every day, there's a new service that wants to use the wireless network. There will be more business needs than available bandwidth," said Horsley.

Even the additional bandwidth that will come with 802.11n upgrades isn't limitless and will only delay the hard choices that will have to be made. "At some point, we'll have to pick and choose what services to run on the network," Horsley said.

The desire to expand the number of services that use the wireless network must also be weighed against increasingly strict security and compliance regulations for patient information. With such critical data on the network, restricting which services use the network, and when, may turn into a sound policy. ■

Stan Gibson is a contributing writer to SearchHealthIT.com. Write to him at editor@searchhealthit.com.

BROCADE

DO YOU NEED TO FREE YOURSELF?

Are network “walls” preventing your doctors and nurses from collaborating effectively? Do you want to work more efficiently and ensure that confidential patient data is completely secure?

Escape to the advantages of next-generation mobility with Brocade® unified wired and wireless solutions for healthcare.

Discover the freedom of innovative Brocade networking solutions at

www.brocade.com/healthcarenetwork

www.brocade.com/healthcarenetwork

CHAPTER 3

NEW GUIDELINES FOR DEVICE SECURITY

When physicians use wireless devices and smartphones, HIPAA and HITECH compliance gets a little sticky. Here's how to plug privacy holes. **BY DON FLUCKINGER**

THE FEDERALLY mandated health IT buildup taking place between now and 2015 puts hospitals in a catch-22. On one hand, interoperability of applications, devices and electronic health record (EHR) systems is forcing networks open, especially with patient monitoring devices, Wi-Fi tablets and laptops—as well as smartphones—requiring more wireless infrastructure. Yet the HITECH Act mandates that health care providers close off networks and maintain better security for Health Insurance Portability and Accountability Act (HIPAA) compliance, and gives wider enforcement powers to state attorneys general in addition to the U.S. Office for Civil Rights.

That means many CIOs are expanding wireless networks while, at the same time, federal rules require them to guard their systems from would-be data thieves more closely than ever before. That calls for risk analyses of everything wireless in the hospital environment, from the network to the access points to the devices connecting to them.

"The data is much more accessible than when it's in a wired network," said Todd Cooper, co-chair of the International Electrotechnical Commission (IEC) Joint Working Group 7, which is developing IEC 80001, a standard for managing risk in wired and wireless health care networks. "Not only do the communications themselves have to be secure, but you have to deploy a whole new level

of security to make sure that these devices are allowed in."

BEFORE FLIPPING THE SWITCH, MAKE A PLAN

Conducting risk assessments not only helps uncover vulnerabilities in wireless networking. It can also strengthen a hospital's case that it took "reasonable steps" to protect patient data and was not "willfully neglectful"—two HIPAA concepts that can result in fines of $50,000 per violation, up to a maximum of $1.5 million per year, when federal investigators determine hospitals are on the wrong side of the law.

Many hospital departments, including safety, disaster management and risk management, use the failure mode and effects analysis (FMEA) technique to conduct risk assessments to uncover weak points in operations. Elliot Sloane, director of Drexel University's health systems engineering program, said the method also can help determine how a wireless network's security could be compromised—and to figure out how to shore up problems before they occur. The federal government's patient safety site offers health care-specific FMEA tutorials for IT leaders new to the methodology.

One FMEA example in a wireless network risk assessment might be to imagine, "What is the worst-case scenario that can happen if a doctor hooks up his home wireless router to our network and a hacker uses this rogue access point as an on-ramp to our EHR system?" From there, one aims to prevent data breaches by either implementing a hardware solution or writing a hospital policy forbidding the setup of such rogue access points—or both.

CONDUCTING RISK ASSESSMENTS NOT ONLY HELPS UNCOVER WIRELESS VULNERABILITIES. IT CAN ALSO STRENGTHEN A HOSPITAL'S CASE THAT IT TOOK "REASONABLE STEPS" TO PROTECT DATA.

There are three ways to solve problems uncovered in risk assessments:

- Engineer them out, which means addressing them with technology or eliminating an offending device or piece of software.
- Create signage that warns of potential problems to users.
- Train employees, which Sloane

characterized as the least effective method.

Whatever risk assessment and mitigation method you choose, Sloane emphasized, make sure it's done for every device used on the wireless network, whether it's a medical device tracking information on patients or a new iPad a physician is using for

Establish Strict WEP Key Governance

WI-FI PROTECTED ACCESS encryption has superseded Wired Equivalent Protocol (WEP) encryption, which has been deemed insufficient for corporate environments. If WEP encryption must be used, it therefore must be subjected to strict governance.

Sloane said some of the hospitals he visits have worse governance than the hotels he stays in. Hotels give WEP keys to guests and change them on a weekly, or sometimes daily, basis. On the other hand, hospitals—charged with securing patient information that courses through thousands of devices and even more access points—have no system for changing WEP keys. Others do, but they don't change them frequently enough.

This practice leaves networks vulnerable to part-time or terminated employees and other unwanted guests, including owners of rental and loaner devices used on the network. All could potentially hijack protected health information.

"I find it fascinating that I can walk into some hospitals without any controls at all and get on their wireless network," Sloane said. "Why is a hospital giving more robust and more convenient access than a hotel? Is that a good thing? I'm not sure I want to be in a courtroom explaining that."

Sloane provided a four-step plan for managing WEP keys:

- **Put someone in charge of governance.**
- **Set a policy for when to change keys.**
- **Oversee the update.**
- **Document it.**

"It requires a lot of planning and synchronization. Most of the medical devices won't be compliant," he said, "but most things that are Windows-oriented might allow that kind of network utility with proper configuration and passwords [to] make those changes." —D.F.

email. Assign a risk score to each device relative to how much patient data it handles and how frequently, and whether it holds or transmits data, or both. Address the highest-scoring problem devices first.

Beyond that, it pays to partition the wireless network. That way, patients or visitors on laptops, tablets and wireless-enabled MP3 players stay away from network areas where patient data is flowing.

ENCRYPT ALL PROTECTED PATIENT DATA

Risk assessment isn't just a one-time exercise. It's an ongoing process from which policies arise—and must be enforced—for compliance with HIPAA to occur.

Encrypting protected patient data can be a safe harbor to avoid HIPAA violations when data is lost—under the HITECH Act's update to HIPAA, if data that is lost is encrypted, the event does not constitute a data breach.

Consider encrypting all protected patient data. This can be thorny on the device level and is leading some facilities to decide that virtual private networks are the most cost-effective way to encrypt. Moreover, many hospitals use legacy systems and equipment not designed to handle data encryption, so integrating data encryption into a wireless network can prove problematic.

However, Cooper said, newer devices such as patient monitors offer HIPAA-friendly features that enable encryption of the data points (such as a patient's name) that the law considers protected health data. That makes it easy for the IT manager, who just needs to make sure encryption is turned on and functioning properly.

RISK ASSESSMENT IS AN ONGOING PROCESS FROM WHICH POLICIES ARISE—AND MUST BE ENFORCED —FOR HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) COMPLIANCE. ENCRYPTING PATIENT DATA CAN BE A SAFE HARBOR TO AVOID HIPAA VIOLATIONS WHEN DATA IS LOST.

Cooper also recommended that CIOs keep an eye on the IEC 80001 standard, which, along with implementation guidance, is due this year.

"The whole point of 80001 is to do risk management for these kind of networks, including wireless net-

works, where you're trying to balance between three key properties—patient safety, system effectiveness and data and systems security. It's in the order of priority, so your priority is risk management to ensure patient safety, No. 1, but also data and systems security," Cooper said. "There's a real tension between those. The safest, most secure medical device is one on the shelf [not in use], but it's not very effective."

THE NO. 1 HIPAA SECURITY AND PRIVACY ISSUE WITH SMARTPHONES IN A HEALTH CARE SETTING IS THEIR BUILT-IN CAMERAS. TO BOLSTER COMPLIANCE, LIMIT OR PROHIBIT THEIR USE.

DEVELOP SOCIAL NETWORKING POLICIES

C. Peter Waegemann, vice president of mHealth Initiative Inc., a nonprofit industry group championing mobile health care applications, said personal email and social networking sites can be venues for HIPAA violations. He offered several pointers for ensuring that what one may think are mobile health innovations don't turn into privacy and security vulnerabilities:

- The No. 1 HIPAA security and privacy issue with smartphones in a health care setting is their built-in cameras. To bolster compliance, limit or prohibit their use. Though public officials might ask to be photographed for public relations purposes, and though it may be tempting to snap shots of celebrity patients, many hospitals prohibit all photography inside their buildings.
- Encrypt all data sent to and from mobile devices.
- Many smartphone apps plug directly into feeds for social media sites such as Twitter and Facebook. Though this makes communication quick and straightforward, facilities nonetheless should ban one-on-one communication about treatment between patients and staff members utilizing social media.

"If you comply with those, if you understand what's going on there, [use of mobile health devices] is, in general, HIPAA compliant," Waegemann said. ■

Don Fluckinger is features writer for SearchHealthIT.com. Write to him at dfluckinger@techtarget.com.

CHAPTER 4

IMPLEMENTING A WIRELESS NETWORK

As if setting up a wireless network wasn't hard enough, hospital CIOs must also contend with medical devices, HIPAA compliance—and microwave ovens.

BY DON FLUCKINGER

SETTING UP or upgrading a hospital wireless network features all the trials and tribulations of the task with which CIOs in other industries are familiar—namely, overcoming low-signal areas, solving spectrum issue and guarding against rogue access points. The objective on the back end is the same, too—maintaining a consistent signal without dead spots that makes it easy to switch from one access point to another and, as a result, reduces the time spent troubleshooting.

On top of that are two challenges unique to health care: There's the constant proliferation of medical devices transmitting wireless signals, which causes bandwidth and spectrum issues in some areas, especially the emergency department. There's also strong security and privacy regulation; noncompliance means a financial penalty running into the millions and a public listing on a government website, both of which can cause immeasurable damage to a facility's reputation.

Done right, though, a wireless network can be a game changer.

"Wireless enables a lot more than mobility in health care," said Patrick Hale, chief technology officer at Sparrow Health System in Lansing Mich., which set up a new enterprise wireless network in a new hospital tower three years ago. "We're still learning the true impact of that, and [it's

already] had a tremendous impact—everything from our emergency department being mobile and achieving better patient care scores to our food service department being able to turn on concierge service."

Hale and Sparrow network manager Jason Loznak are applying the tower's wireless topology to satellite facilities on multiple campuses, where they are ripping and replacing the existing network to support a new rollout of Epic Systems Corp.'s electronic health records (EHR) system. Sparrow anticipates caregivers will use Epic heavily on wireless devices. Already in the new tower, wireless is improving Sparrow's patient experience in a number of ways—physicians access the EHR system on tablets, patients order meals from their beds and nurses admit patients at the bedside.

BUILD AN IMPLEMENTATION PLAN

Setting up a wireless network starts with a strong implementation plan. Loznak said the first thing to do is select a hardware vendor. Sparrow ultimately used Meru Networks Inc. Other vendors to consider include Cisco Systems Inc. and Aruba Networks Inc.

Determining the best fit involves more than listening to sales pitches. Loznak recommended testing a vendor's gear to get a feel for how well it works in your environment and with the devices your hospital network supports, be they laptops and tablets or wireless patient diagnostic tools or infusion pumps.

> "YOU REALLY WANT TO BATTLE-TEST YOUR CURRENT CLIENT ENVIRONMENT AGAINST THE [NETWORK HARDWARE], IN A LIVE ENVIRONMENT, TO FIND WHAT KIND OF ISSUES YOU'RE GOING TO BE DEALING WITH AFTER GO-LIVE."
>
> —JASON LOZNAK, network manager, Sparrow Health System

"Every vendor will come in and tell you they're device-agnostic, everything will work on their product. It's just flat not the case," Loznak said. "Some things are going to work much, much better than others. You really want to battle-test your current client environment against the product, in a live environment, to find what kind of issues you're going to be dealing with after go-live."

Get a feel for a wireless vendor's software network management tools.

In Hale's view, this is a key differentiator. These tools have improved significantly during the past few years, from rudimentary dashboards to more sophisticated utilities, he said, but even the best in class could use some improvement.

HEED SITE CONSIDERATIONS

Once you have decided which vendor will supply your wireless network, plan for its implementation. Determine what areas of the facility it will cover, and what the workflow inside those areas looks like. Key considerations include what devices staff will use, how mobile the staff is, and whether interference, from something such as a radiology lab, will be a concern.

"If this is your first install, I would highly recommend spending the money to bring somebody in that's got the back-end experience at many, many other locations, who has seen a lot of gotchas you aren't prepared for," Loznak said. It comes down to "yourself, vs. someone who's done several hundred of these."

Issue a request for proposal and collect responses as you would for other network projects. But also talk to your peers about the integrators who respond, and ask about their experiences with them.

You should be "very particular" about integrator selection, Loznak said. "You want to not only focus on their technical prowess and capabilities, but you also want to put some keen focus on their project management capabilities."

Wireless network integrators who are organized and deadline-driven will help you meet your timelines, recover from challenges and roadblocks that inevitably arise during the implementation process, and work with manufacturers when defective or malfunctioning hardware comes in.

Part of that integrator evaluation is how the company does a site survey. Loznak recommends avoiding computer models of your site, except for ballparking costs. These models fail to take into account impediments that might weaken wireless signals—or, as Loznak described them in referring to his room-by-room, physical site survey, "weird areas." Such areas include medical records rooms filled with three-feet-thick walls of boxes full of paper, other bookcases, pipes not shown in the building schematics, and bathrooms on top of bathrooms on multiple floors.

CONSULT WITH EVERY DEPARTMENT

A spot that would provide a strong wireless signal may not be ideal for other reasons, as well. If, for example, an access point malfunctions in a

room where infection control precautions are in effect, how do you fix it? Can you situate a router in a place where it optimizes signals from within a high-efficiency particulate air tent and is simple to replace or repair? These are questions only your infection control office can answer.

Safety managers will have their concerns, too, and the facilities manager will have tips for protecting gear from air-handling units. You will spend a lot of time determining placement for access points and their power supplies that simultaneously are easy to maintain but do not interfere with heating and air conditioning, as well as with patient care.

It's an arduous but necessary process, best accomplished with all stakeholders at the same table, Loznak said. That way, physicians in, say, the neonatal intensive care unit or the post-anesthesia care unit "understand exactly what you're doing" and why it's important.

Hale concurred: "It's critical. It's just dangerous if you don't that you take those steps."

TECHNOLOGY, POLICY WORK TOGETHER

Spending money, unfortunately, is part of how to get a wireless network ready for an EHR system, Hale said. It's a tough sell, but it's important to convince the hospital board of directors to invest in a solid wireless infrastructure and support it from the beginning—either that, or suffer a painful outage later when patients' lives are on the line.

IT'S A TOUGH SELL, BUT IT'S IMPORTANT TO CONVINCE THE HOSPITAL BOARD OF DIRECTORS TO INVEST IN A SOLID WIRELESS INFRASTRUCTURE AND SUPPORT IT FROM THE BEGINNING.

Even after the upgraded network in Sparrow's hospital tower went online, problems cropped up. They continue to do so, which leads to another piece of advice from Hale and Loznak: Plan for wireless implementation to be an ongoing process. You may have to move or add an access point around a high-traffic area such as the emergency department so signals don't drop as harried nurses carry their tablets from one room to another.

In addition, diagnose and work around a persistent problem that causes service call after service call. This isn't always easy. Monitoring tools can't re-create what was happening in a room when a problem

was reported—and by the time IT staff arrives, things can revert to normal.

For Hale and Loznak, the problem was "microwave alley," a group of five employees who all have microwave ovens at their desks that negatively affect the wireless network around lunchtime.

"We went in there with RF studies, [and] it was fine," Hale said. "It was one of those really frustrating, intermittent—but when it happened, really serious—wireless problems."

Eventually, with some outside help, they traced the problems to the microwaves. While diagnosing the problem was one thing, solving it has been a different matter. "We're still fighting the battle to get rid of those microwaves," Hale said with a laugh.

That brought him to one final tip for a successful hospital wireless implementation—give users a realistic explanation of what to expect in a new wireless network. Performance, and experience, will vary.

"Tell them [that], from time to time, even the best wireless networks will drop you," Hale said. "It doesn't mean there's anything wrong. It just means that's the price you pay for mobility. There's no truly, completely bulletproof wireless network." ■

Don Fluckinger is features writer for SearchHealthIT.com. Write to him at dfluckinger@techtarget.com.

SearchHealthIT.com

Engineering the Wireless Hospital
is produced by CIO/IT Strategy Media

Jacqueline Biscobing
Managing Editor

Linda Koury
Art Director of Digital Content

Stan Gibson
Contributing Writer

Don Fluckinger
Features Writer

Brian Eastwood
Site Editor

Anne Steciw
Assistant Site Editor

Jean DerGurahian
News Writer

Scot Petersen
Editorial Director

Rachel Lebeaux
Assistant Managing Editor

FOR SALES INQUIRIES
Stephanie Corby
Associate Publisher
scorby@techtarget.com
(617) 431-9354

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com

FROM OUR SPONSOR

- **Wi-Fi Provides Rx for Healthcare Challenges Whitepaper**
- **Understanding the Concept of Client Health Score Solution Brief**
- **New Version of Free Wi-Fi Planning Tool**

About Aerohive Networks:

Aerohive Networks, the leader in next-generation enterprise wireless LANs, unleashes the potential of enterprise Wi-Fi, enabling customers to stop buying copper, to move applications to the air, and to maximize workforce productivity.

The company's award-winning cooperative control architecture eliminates costly controllers, saving money and providing unprecedented resiliency, up to 10X better application performance, and an opportunity to start small and expand without limitations.

FROM OUR SPONSOR

BROCADE

- Brocade Healthcare Network Solutions
- IP/Ethernet Solutions
- Healthcare Customer Success Stories

About Brocade:

Brocade® (Nasdaq:BRCD) develops extraordinary networking solutions that enable today's complex, data-intensive businesses to optimize information connectivity and maximize the business value of their data. For more information, visit www.brocade.com/healthcare.