Making Wireless Work

A Look at What Hospitals Are Doing

Martha Vockley

Three events in January 2016 did a terrific job of capturing the essence of wireless technology in healthcare today, putting the expectations, innovations, and problems in the limelight. In glitzy Las Vegas, more than 150,000 people flocked to CES (formerly the Consumer Electronics Show) and the colocated Digital Health Summit. An equally engaged crowd of 1,000+ health information technology (IT) and healthcare technology management (HTM) professionals gathered in Cleveland for the IHE North American Connectathon.
CES stoked consumer expectations for the latest and greatest gadgets, including wearable, mobile, and wireless technologies for health, fitness, and, yes, medical applications. The poster child this year: MedWand, a handheld device that captures vital clinical data at home for video telemedicine consultations with a physician—and records those data in a secure medical record compliant with HIPAA (Health Insurance Portability and Accountability Act). The device won the prestigious 2015 Health 2.0 Launch! Award and earned a spot on Frost & Sullivan’s top 10 list of disrupters in healthcare.

At the Digital Health Summit, thought leaders in healthcare, industry, and academia focused on how innovative consumer and medical-grade technologies—and the data they generate—are shattering traditional models. Digital health is reshaping healthcare delivery, redefining caregiving, empowering patients and caregivers, personalizing medicine, and much more.

The Connectathon injected a dose of reality into the increasingly wireless world of healthcare technology. There, tech professionals engaged in connecting healthcare systems and devices and putting them to the test for safety, effectiveness, and security. Participants also sharpened their skills for managing the health IT infrastructure, where wireless and wired technology coexist—a skillset that is in high demand.

That’s the reality that health IT and HTM professionals are living every day. How exactly do they make wireless work in their healthcare systems? How do they meet rising expectations, advance the promise, and solve the problems? And how do they keep their skills up to date?

To find out, we turned to members of the AAMI Wireless Strategy Task Force, which is working to:

- Clarify roles and responsibilities in wireless technology management.
- Offer guidance in managing the spectrum to improve safety, reliability, and security.
- Provide guidance on managing risk, preventing failure, improving security, and preventing cyberattacks on medical devices.
- Address the supportability of wireless connected devices.

Facing both common and unique wireless challenges and opportunities, wireless experts at Johns Hopkins Medicine in Baltimore, MD; Baylor Scott & White Health in Dallas, TX; and Henry Ford Health System in Detroit, MI, are working strategically to address them.

Enterprise Wireless Standard Guides HTM

“The biggest challenge I have in front of me right now is securing medical devices and segmenting them on our medical networks,” said Calvin Sproul, network manager for wireless technologies at Johns Hopkins Enterprise. That challenge encompasses securing patient health information and creating an internal separation between open- and closed-access networks. Both mobile medical and consumer devices—including off-the-shelf devices, such as tablets, that clinicians are using to practice medicine—are in the mix.

This initiative builds on IEEE 802.1X, a network standard that is the basis for WPA2-Enterprise security for authentication and encryption of network device access and data transmission. Johns Hopkins has been using this standard for some time. “We’re picking this point to start our really granular segmentations to our clinical networks for wireless—to control what kind of access people have to applications like an EMR [electronic medical record],” Sproul said.

“The big focus right now is encrypting local storage on the device, in case that device is lost or stolen,” Sproul added. “This is for all devices, not just mobiles, but it just so happens that medical devices are moving around so much more. Once you start to connect these devices to networks, it makes them much more powerful. The collection of information is much more robust. But they’re also more vulnerable. Also, when you understand how these things connect, you start to reap the benefits of efficiencies and scale. One person can therefore manage more devices more effectively.”

To undertake this initiative, Johns Hopkins has an unusual resource in hand—an enterprise wireless standard incorporated into the system as policy. The 24-page document covers best practices and guide-
lines for wireless medical devices, clinical and institutional system integration, and clinical communications. Among other topics, Johns Hopkins’ Clinical Wireless Device Standard identifies the technical standards, spectrum frequencies, and encryption methods that Johns Hopkins uses, as well as procurement and project management policies for new wireless technologies.

The standard also provides practical tools, such as questionnaires for vendors that can be turned into matrices for evaluating new technologies. Three of the big requests for vendors:

1. Use a dual-band adaptor
2. Incorporate an adaptor into the medical device itself, with no bridges (e.g., don’t take an existing Ethernet port and bridge it over into the enterprise wireless radio)
3. Use WPA2-Enterprise encryption (the most secure available)

“I didn’t see that there was any form or order to the way that we were bringing in medical devices—wireless was just being bolted on to existing medical devices. It was all over the map as far as security.”

—Calvin Sproul, network manager for wireless technologies at Johns Hopkins Enterprise

These aren’t trivial requirements, Sproul said, though at least some vendors are willing to try to meet them.

“And then we’ve got a list of 11 or 12 ‘thou shalt nots,’” Sproul said. For example, “Even though I can put a variance on something, I don’t want to see a bridge or some kind of ‘bolt on’ just to make something wireless, say an ultrasound machine.”

Experiences like that, in fact, prompted Sproul to write the standard, which was approved by the healthcare system’s policy and standards committee.

Another major healthcare system, Kaiser Permanente, based in Oakland, CA, developed an enterprise-wide wireless standard several years ago as well. “We needed a way to have clear requirements for project teams procuring wireless devices,” said Shawn Jackman, formerly director of strategic planning at Kaiser, now founder and CEO of Clinical Mobility, as well as a member of the AAMI Wireless Strategy Task Force. “Wireless is one of those technologies where you can’t tweak the network infrastructure for every device. Many configuration components are global and affect all devices. Effectively, you have to develop an infrastructure standard and adapt devices to the design framework. It is complicated.”

**Change Management**

**Patch Management.** The Johns Hopkins standard and business practices address protocols for managing changes to wireless networks—a growing challenge for healthcare systems.

Software and hardware changes are discussed in a “morning call” that occurs every weekday among enterprise IT staff and those who are effecting or affected by a change. This vetting and coordination by peers happens “whether it’s a midrange system, our virtual systems, our VMware, our mobile device management, our EPIC (EMR system), or other medical systems or applications,” Sproul said.

A change control coordinator approves changes and has the authority to determine whether a change is risky enough to require more stakeholder involvement or further risk analysis. Approved changes are scheduled so they do not conflict or interfere with other changes. Significant changes that could affect the enterprise or an entire hospital could require C-suite, or senior executive, signoff. For such changes, staff members are alerted in advance.

“So for example, I have a change in for tonight for our distributed antenna system,” Sproul said. “I need to test one of the base units, I need to bring stuff down. Well, I had to coordinate that with our other communications systems, so that we don’t
impact our clinical staff too much with communication troubleshooting. If somebody complains of a communication issue, we would know which system was impacting it.”

The lack of good patch management, and patch management services for medical device systems, is a “pet peeve,” Sproul said. “If I have to push a patch to medical devices once they’re on the wireless network, or update the security or certificate of something like that, I don’t think there are really any good systems to do that. This is also a pet project that I would like to see developed.”

Security Requirements, Guest Expectations

Like Johns Hopkins, Baylor Scott & White in Texas is in the midst of securing access and data from wireless medical devices and segmenting those devices on its networks. At the same time, the health system is redesigning its wireless guest network. These challenges go “very much hand in hand,” said Alex Moore, wireless network expert there.

Baylor Scott & White’s quest to keep access and data secure illustrates the fast-paced changes in wireless environments. “The Wi-Fi world changes faster than almost any other aspect of the networking world,” Moore said. In just a couple of years, the healthcare system has upgraded the security protocols that wireless medical devices use to connect with the wireless network and feed data to back-end servers.

“There are different security methods for that,” said Richard Swim, team leader for clinical technology. “It goes all the way back to simple security—which is no security. Anybody and everybody can get on the network if it’s configured to talk to the SSID [service set identifier, the technical name of the wireless network] or the wireless LAN [local area network]. We’ve never done that here. But we’ve gone through different phases of security,” beginning with WEP [wired equivalent privacy], “which was first touted as being very secure and was cracked within days after it was released.”

Next, Baylor Scott & White moved on to WPA [Wi-Fi protected access] Personal, which is encrypted, but uses a common passkey. Assigning a common passkey to multiple devices, as do wireless home networks that typically use WPA Personal security, is problematic in a healthcare institution, Swim pointed out. If the passkey is compromised, all devices are compromised and the network could be breached.

Now there’s WPA2-Enterprise, which supports specific security credentials, such as a certificate or user ID and passkey, for every device. “That sounds pretty secure and it is,” Swim said—but devices can still be compromised. “An organization can limit a single device user ID and password on the network at one time, that’d be nice. The other thing that can cause havoc there is, what do you do with those passwords? And how do you issue them for 5,000 infusion pumps that you may have in your organization, which is what we have here in North Texas? That’s a documentation nightmare and a security nightmare, trying to generate the passwords and then keep them safe to where they’re used on the medical device at the time of configuration and then kept secure after that or destroyed.

One method you could use is to configure the device with a user ID and password and then, basically, throw the password away. The device should never forget that. If it ever has to be reconfigured, a unique user ID and password could be regenerated. That’s what we’re wrestling with right now.”

For some devices, Baylor Scott & White opts for the enterprise version of WPA Personal, often referred to as PSK [pre-shared key] encryption. Clinician workflow drives that decision. “If it’s a device that’s going to be shared by multiple team members, such as an IV pump or a team workstation or laptop, then typically we set it up as a pre-shared key,” Moore said. “If it’s a device that only one person is going to be using and it doesn’t impact their workflow, then we will set it up as WPA-Enterprise.”

WPA Enterprise authorization makes it easy for clinicians to get on the network quickly, but there is a drawback. If someone repeatedly enters the login information incorrectly, the Windows Active Directory will lock...
down all of the devices that use the same login information. “That makes for a very bad day for those nurses and doctors,” Moore said. “It’s a bit of risk for us but one that we have documented.”

Migrating wireless medical devices to more robust authentication protocols can be a challenge. “Think about how fast the network changes and how medical devices don’t change that often,” Swim said. “The medical devices we get are typically two- to three-year-old technology right off the bat when they’re brand new.” It can take that long to secure FDA approval or clearance and get products to market—and it takes time and money to purchase new devices. So Baylor Scott & White finished migrating devices off of WEP protocols only recently.

“Guest Access: From Courtesy to Mission Critical
In recent months, guest access has eclipsed virtually every other wireless challenge at Baylor Scott & White for reasons spanning security, access, guest satisfaction, reimbursement—and clinical practice.

On the security front, Baylor Scott & White’s security department raised concerns about guests using the same wireless network as medical devices—and, potentially, accessing devices and anything else on the enterprise network. For example, “in our Plano hospital, they’re connecting to a wireless antenna out on the 10th floor,” Moore said. “That antenna is connected physically to one of our network switches. There are connections from that particular switch all the way back to our core network, over to our data center and everything. They’re riding the exact same network switch that our nurse station computers are connected to.”

At the same time, guests now expect robust, uninterrupted Internet access on their personal devices—and they complain if they don’t get it. Say a patient is receiving radiation therapy. “When they get out, they actually ding us on the review because they didn’t have adequate Wi-Fi,” Moore said. “They couldn’t stream Netflix, it wasn’t in HD. They’re completely disregarding the fact that this awesome radiation machine was able to shoot radiation into their body and remove the tumor that’s been causing them medical issues. The medical care is taken for granted.” That’s been an eye-opener. Guest access has been viewed as a courtesy, an “afterthought” compared with Wi-Fi access for medical technology and administrative uses, according to Moore. Not anymore. Patient reviews factor into reimbursement, which is of course a high priority, as well as into patient and family choices when it comes to healthcare.

Moreover, “guests” aren’t just patients and visitors. Clinicians bring their own tablets and smartphones to work and expect to jump onto clinical systems and the Internet just as expeditiously as they do anywhere. In several cases, physicians have used the guest network for medical procedures, such as an off-site streaming video consultation by a visiting physician via a webcam on a personal laptop. “They’re using this network outside of its intended design,” Swim said. This shouldn’t happen—and the health system’s network experts do their best to make sure physicians understand the limitations of wireless networks—but sometimes, it does.

As a result, “we’re having to redesign our wireless guest network and not treat it quite as the stepchild it had been in the past,” Moore said. In addition to segmenting the network for medical device security, this entails ensuring that Baylor Scott & White’s large wireless environment—which includes 70 wireless controllers and upwards of 30,000 guest, medical, and corporate devices in use daily—can handle all of the traffic.

Staff use of personal devices brings another challenge: password management. As a security measure, Baylor Scott & White periodically changes staff usernames and passwords for wireless network access. Clinicians and other staff members don’t always remember to change their saved login information on their personal devices. So their enterprise accounts lock down if they attempt to log in with old credentials. Staff members don’t always remember that they’ve even used personal devices to access the enterprise wireless network, which led to plenty of time-consuming, back-and-forth interactions with technical support staff.
For this reason, Baylor Scott & White updated its intermediary server, which mediates communication between the wireless network and Windows Active Directory domain controllers. The new architecture provides detailed logs of specific usernames, passwords, and enterprise and personal devices that attempt to log on to the networks, as well as their locations. This enables quick identification of personal devices that staffers might need to update with valid login information.

**Benefits of Leveraging Wireless Infrastructure**
Beyond security projects, Baylor Scott & White is leveraging its wireless infrastructure for a real-time location system (RTLS), which tracks assets such as medical devices and people. To do this, the healthcare system is working with its vendor to build on its existing wireless access point (AP) infrastructure.

“With that, we discovered that we needed to change the way we lay out access points so there’s more triangulation of signals, so we can locate devices on a floor plan more accurately,” Swim said. In the past, network designers would lay out APs straight down hallways, avoiding patient rooms, for ease of installation and service. It turns out, however, that today’s APs rarely need servicing, so concerns about disturbing patients and disrupting care in patient rooms have diminished.

Thus, all new construction and renovations now use a “checkerboard” style of AP placement, including patient rooms and extending to the edges of buildings, where spotty wireless coverage can be a problem, Moore said. That’s the design throughout Baylor Scott & White–Waxahachie, a medical center that opened in December 2014. The APs there are primed for the next wave of super-fast Wi-Fi running on the 5 GHz band of spectrum, which uses the IEEE 802.11ac wireless networking standard.

“There are side benefits to this,” Swim said. “It helps improve wireless coverage for the guests,” who are typically on the edge of the buildings in patient and visitors rooms. “Plus, we use Voice over IP [Internet Protocol] for our caregivers, our nurses. That improves the wireless coverage for those telephones as well,” along with medical device connectivity and clinician traffic on the wireless network.

Anecdotal reports from guests and clinicians indicate that the Waxahachie wireless environment is operating very well compared with the Wi-Fi in facilities with older systems, Moore said. That success just raises the bar higher, however. In fact, some physicians no longer want to practice in facilities with wireless connectivity issues.

**Throwing the ‘Frankenstein Switch’**
Given the accelerating industry consolidation of healthcare systems, the wireless implications of the merger of Baylor Health Care System in north Texas and Scott & White Healthcare in central Texas into Baylor Scott & White are instructive.

While the merger was officially completed in 2013, the wireless “kumbaya” has been happening only within the past year or less, Moore said. The seemingly straightforward change-of-address task is more challenging in the wireless world than it is in the physical world. Every device that wants to use the Internet needs an IP address. Some devices use dynamic IPs—the wireless network server automatically generates and sends an available IP to these devices every time they try to access the Internet.

Other devices don’t have that capability. They use static IP addresses that are configured into them. With the merger, some devices with static IPs in the formerly separate organizations used the same IPs, which meant that the addresses needed to be changed so that the enterprise network would not be confused by duplicate addresses. “You have to physically go and find them and reconfigure them,” Moore said. “Sometimes it was entire systems. Radiology devices are notorious for that.

“The way Wi-Fi operates, I have to do all of the reconfigurations at one time,” Moore explained. “So in terms of the corporate wireless in Plano, we have three wireless networks—corporate, medical, and voice. It’s like a big Frankenstein switch. Basically I have to throw the switch to turn off the corporate wireless, reconfigure the IP address and the IP network it’s going to use, and then turn it back on again.”

Technically, that’s not necessarily a heavy lift—though some devices don’t take to reconfiguring without some hiccups.

**Expert Perspective**
Shawn Jackman, founder and CEO, Clinical Mobility

“Wireless is now the primary network. Wireless speeds are so high now it’s no longer an issue.

“Many devices do not even have a wired port anymore. Provisioning wired ports and running physical cables is a cost. You eliminate all of that with wireless in that you only configure it once. Wired ports are finite and are expensive to expand with business needs.

“Also, wireless isn’t just for mobile devices anymore. Then, we have the Internet of Things (IoT), which is a massive onslaught of wireless device expansion. To some who are less involved in watching this massive momentum shift, wireless is sometimes viewed as a secondary and nice-to-have solution. Yes, this is legacy thinking, but it is often inside the minds of some staff, which may include management.

“Wireless is one of the most strategic IT assets that enables clinical workflow and staff communication, patient satisfaction and experience, locating people and devices, temperature monitoring, and building systems. It must be done with high performance and high levels of security in our highly regulated industry.”
Clinically and logistically, however, reconfigurations can take hundreds of devices offline at once. That requires “massive coordination” with everyone—and no one is particularly happy at the prospect of wide-scale downtime.

For some medical technology, averting data loss during reconfigurations is paramount as well. For example, Baylor Scott & White is in the midst of changing the address range of a wireless telemetry system in some hospitals—and trying to do this without losing any patient waveforms. A test run at one hospital didn’t work, so the experts regrouped. “The planning that led up to this change has already taken countless hours,” Swim said. “Trying to minimize the impact to the clinicians is going to take countless hours more. So this takes hours and hours and hours of planning for something that might take five minutes to implement.”

Beyond this address change, the merger also has resulted in a standardization of the setup of the wireless telemetry system enterprise-wide. “We’ve chosen to separate our patient waveforms on a WMTS [wireless medical telemetry service] system,” Swim said. This system runs on 1.4 GHz, rather than the 2.4 and 5 GHz used by the enterprise wireless. That protects the telemetry system from interference from changes to other devices.

### Wireless for Mobile Health and Innovation

For Ali Youssef, senior clinical mobile solutions architect at Henry Ford Health System in Michigan, mobile health, telemedicine, and home care represent huge opportunities to solve the biggest challenge in healthcare: costs that are not sustainable. All of those solutions rely on wireless technology, which supports care for patients wherever they are—and keeps them out of hospitals.

Right now, the sheer volume of wireless medical devices, consumer devices, and apps in two different arenas—inside and outside of hospitals—is consuming the management bandwidth at Henry Ford.

“The biggest challenge is basically being able to meet all the best practices from a technology perspective as well as the governmental mandates for things like security, ensuring patient data is secure, ensuring that your experience is repeatable, that you’re getting a high quality of experience over and over again,” Youssef said. “We have so many technologies that are trying to play in that same space and are being introduced into the hospital setting and the healthcare setting. Getting the technologies to coexist and not to disrupt each other, that’s going to be the biggest challenge.”

For the past few years, Henry Ford has focused on mobile medical devices. “We ran into several issues with devices from fairly prominent medical device manufacturers that just did not meet the appropriate specifications—at least our specifications—which are aligned with best practices,” Youssef said.

That’s a problem across the healthcare community. “This is so common for devices to have issues that it is nearly assumed by those of us who deal with networks,” Jackman of Clinical Mobility said. “In fact, we are surprised when a device doesn’t have a problem.”

At Henry Ford, health IT and HTM professionals developed a device certification and onboarding process for wireless medical devices. “We essentially ask a series of questions that have to do with the functionality of the device, security, how well it roams if it’s leveraging the Wi-Fi network,” he said. “If it’s leveraging other spectrums, we need to make sure it can coexist with other types of devices in the hospital.”

The idea is to understand and document the risks upfront, with a feasibility study by wireless and security teams, as well as HTM professionals and clinicians, before a device is purchased and deployed. This technical analysis includes functional testing, network testing, and fail-over and redundancy testing. The testing team asks such questions as:

- What happens to a device if the Wi-Fi network or mobile network it’s dependent on is disrupted or offline?
- How does the device react? How does it recover?
- What happens to the data?

“You have to scrutinize each and every device,” Youssef said. “I’ve run into mobile X-ray units where, if you want to switch the device from being a mobile unit to actually
A Touchstone for Making Wireless Work: ANSI/AAMI/IEC 80001

Johns Hopkins, Baylor Scott & White, and Henry Ford are all making use of the standard ANSI/AAMI/IEC 80001 to manage risks associated with wireless technology networks. For example:

- Johns Hopkins considers itself an early adopter of 80001. Its enterprise wireless standard incorporates many standards, practices, and documents from 80001—and that standard is policy throughout the healthcare system.
- Baylor Scott & White’s change control processes align with 80001, and its close relationships with key vendors reflect best practices in terms of shared responsibility for managing networks.
- Henry Ford’s risk assessment aligns with 80001, as does the next “really important” step in the process—putting in place an operating-level agreement that formalizes responsibility for procured devices. “Literally, it’s almost a support contract that defines who supports different pieces if this device were to break down or malfunction,” Youssef said.

Still, none of these healthcare systems has fully implemented 80001. Two sticking points prevail. First, the standard seems at first to entail a significant, systemic undertaking and considerable changes in practice, with no clear signals that current risk management methods are broken. Second, the standard requires healthcare delivery organizations to have a dedicated medical IT-network risk manager, which they are hesitant to do.

Scripps Health broke down the first challenge by focusing its 80001 efforts on a single system, a new wireless telemetry deployment in a new hospital. The four-phase project included:

1. A readiness assessment of key stakeholders for managing IT network risks, which is included in the standard
2. A targeted risk assessment of the wireless telemetry architecture, which included training about network risk management
3. A reassessment of managing IT network risks, which showed a 3X improvement
4. A new 80001 improvement plan focused on physiological monitoring in the post-anesthesia care unit at a different facility

For this project, Scripps Health partnered with the Center for Medical Interoperability (C4MI), which provided valued technical assistance and facilitation for the readiness and risk assessments.

“The driving force for this project for the IT department was security,” said Marcia Wylie, senior director of biomedical engineering, Scripps Health. “For us, it’s patient safety and effectiveness.

“80001 has all three of the key properties—safety, effectiveness, and security of data and systems,” added Scot Copeland, clinical systems specialist and biomedical engineering lead, Scripps Health/Mercy Hospital.

Implementing 80001 wasn’t as hard as they thought it would be. “We discovered that we were not starting from zero,” Wylie said. “We had a lot of practices in place already. We just needed to tie them together, change some policies. You don’t need to invent a whole structure called 80001.”

The 80001 process helped Scripps identify safety gaps, such as the potential loss of data and intermittent loss of communication on nurses’ portable phones, by which nurses monitored patients via telemetry. “That was worth the process of admission for me right there,” Copeland said.
connecting it to an Ethernet jack, you need to reboot the unit, which takes several minutes.”

The certification and onboarding process also heads off duplication of efforts. “From a clinical workflow perspective, in some cases we have several devices doing the same thing,” Youssef said. “There’s really no need for that. It’s better to standardize on one type of device.”

Henry Ford classifies mobile medical devices into three tiers:

- Type 1: non–life-sustaining devices that do not transmit or receive clinical data that includes protected heath information
- Type 2: non–life-sustaining devices that transmit or receive clinical data that includes protected heath information
- Type 3: life-sustaining devices

“"A key trend we’re seeing now is the large number of medical apps. One thing people don’t often think about is that you can design a really good application, but it relies, number one, on your infrastructure as well as the platform it’s running on.”
— Ali Youssef, senior clinical mobile solutions architect at Henry Ford Health System

At this point, Type 3 devices that rely solely on network connectivity to function, and thus could cause direct harm if they were to lose connectivity, are not permitted by the healthcare system.

Mobile medical devices are largely a “finite inventory,” in Youssef’s words, which made them a good place to start standardizing practices. Within the past year, Henry Ford established a multidisciplinary mHealth Advisory Council, which is oriented to mobile health with an “application-centric” focus. The advisory council includes technical subject matter experts, security experts, the chief medical information officer and other leaders, and clinicians.

“A key trend we’re seeing now is the large number of medical apps,” he said. “One thing people don’t often think about is that you can design a really good application, but it relies, number one, on your infrastructure as well as the platform it’s running on.” It’s important to test applications to make sure they function properly on the device for which they are intended.

Related to the influx of mobile devices and apps is the virtual private network (VPN) model of using the Internet to connect to the enterprise network and access data remotely. Based on the number of use cases and the number of devices that are requiring this type of connectively now, better models are needed to be able to scale these networks.

Creative Applications of RTLS

Henry Ford is just beginning a new wireless project that will leverage RTLS, which is used for asset tracking and management, in both traditional and innovative ways. The system uses passive and active radio-frequency identification (RFID) tags, typically to locate devices and equipment.

At Henry Ford, this wireless technology might eventually be used to support:

- Temperature monitoring in sensitive areas, such as surgical suites.
- Stress badges (the demand for an object over time, or workload).
- Security use cases.
- Hand hygiene.
- Clinical workflows, “the ultimate end game to make sure they’re as efficient as they can be.”

In the emergency department, for example, the RTLS system could be used to monitor patient wait time, so no patient is forgotten in a hallway. And it could trigger an alert if patients with mental health issues or other medical conditions try to leave the emergency department, which could endanger themselves or others.

“We’re using different types of technologies to try to accomplish this,” Youssef said, including multi-mode technology that can leverage Wi-Fi for smaller clinics and newer hospitals and a 900 MHz system for larger, older hospitals. “What’s really important about this project we’re initiating now is that it’s setting a standard for the health system.”

Finally, the Henry Ford Innovation Institute, which operates like a startup company, is dedicated to exploring creative ideas in healthcare and other industries. The institute is helping the healthcare system think through the possibilities of wearable devices for medical and health applications.
References


