A Roundtable Discussion

Wireless Ahead: Integrating Medical Devices Into IT Networks

Mary K. Logan, Moderator

For decades, medical devices functioned as standalone products. Then, manufacturers introduced proprietary networks that allowed some devices to share information. Now, those proprietary networks are being eliminated and instead medical devices are being linked together via a hospital’s main information technology (IT) network. This move to integration has recently been made even more complicated by the push to integrate wireless technologies into devices and networks. Here, a panel of experts discusses the challenges and opportunities for healthcare facilities in adopting such technologies, and what resources are available—or needed—to point the way.

Bob Alberte

Clearly the integration of medical devices onto IT networks is the direction things are moving. This integration reduces infrastructure costs and allows better access to data. We all want to use the technology that’s best for our patients, and getting data to the right place at the right time is part of that process. Without some form of integration within the hospital, you can’t do that. The hospital is a very mobile environment. Caregivers and patients are constantly moving around. We need ways to combine the information from these multiple systems into one. Utilizing hospital IT infrastructure is a way to provide that accessibility of data at reduced cost.

Ed Cantwell

There is an overarching desire for mobility within the hospital, and eventually out of the hospital. Wireless technologies offer the power of ubiquity and the power of mobility.
Tom Judd There is a growing demand for wireless capability for medical devices at various levels of care—not only acute care or step-down care in a hospital, but also in ambulatory care. However, we just don’t have the wireless infrastructure in these buildings yet to support all the places we might want to use it.

Don Witters The promise of wireless technology is almost limitless. Much innovation, research, and new product development is enabled via wireless technologies. Wireless is an enabler of mobility—of larger use and more efficiencies and better information flow. Many uses of wireless technologies in healthcare involve relatively low risk and are now being implemented quickly, easily, and cheaply. But some medical functions that present greater risk—drug delivery, therapy delivery, even higher-risk types of imaging technologies—really need to be addressed through risk management. For medical uses, wireless technology needs to be designed, developed, tested, deployed, used, and maintained to perform reliably and securely so that it can improve healthcare and make it more efficient. However, if wireless technologies are not coordinated correctly from the beginning, problems can ensue.

Mary Logan What problems are we seeing with implementation of wireless technologies in healthcare facilities?

Rick Hampton First, wireless technologies are not very well understood. Too many people see wireless technology as the only way to accomplish connectivity, but they don’t always think through what they’re trying to do, how they can get there, or whether there are ramifications. When people think they have to have wireless at any cost, they can wind up creating conflicting systems.

Second, commercial wireless technologies are still works in progress. There are significant gaps in managing large wireless networks to ensure their reliability. When you’re building medical devices with wireless capabilities and running them on a wireless network, you have
Medical applications of wireless technologies require a different level of reliability than consumer applications. So what appears to work just fine in the consumer world is not nearly sufficient in the healthcare world where we are expected to be delivering coverage all the time.

Bob Alberite In the consumer world, we are accustomed to walking into public places and connecting our off-the-shelf phones and laptops to the Internet. This ease of access may have resulted in our guard being lowered to the complexities and concerns of a hospital wireless connection. In reality, designing, deploying, testing, and maintaining a wireless infrastructure in a hospital environment for critical and dynamic traffic is complex and requires a lot of rigor.

Steve Baker Medical applications of wireless technologies require a different level of reliability than consumer applications. For most people’s cell phones, wireless just works most of the time. It’s usually okay if your computer reboots to reestablish Wi-Fi access or if you don’t have Wi-Fi coverage when you go from meeting to meeting. However, it is not okay in the hospital during patient transport to lose coverage on that patient. So what appears to work just fine in the consumer world is not nearly sufficient in the healthcare world where we are expected to be delivering coverage all the time.

Proprietary technologies are also a problem in medical applications of wireless. Wi-Fi vendors all have Wi-Fi solutions and differentiating features such as radio managers that select channels and power levels. As their system makes these adjustments, it sometimes has adverse effects on patient monitoring. For example, if an enterprise Wi-Fi network wants to scan to find a better channel, it has to leave the current channel, which means it can’t support its client, which means data doesn’t get through. That’s an issue that multiple medical device manufacturers have seen on multiple wireless local area network (WLAN) vendors’ products.

Some Wi-Fi vendors have marketed “medical-grade networks” for years, but they have only recently begun system testing with medical devices, and even then, only a modicum of testing can be done by the Wi-Fi vendor. There is often an assumption that if one medical device is validated for operation on a certain network, then all medical devices will work on that network. Another medical device will have different software including a different MAC (Media Access Control) layer, so validating one medical device for a network does not mean that network will support any/all medical devices. That is not clear to most hospitals and IT vendors. No one but the medical device manufacturer can validate its own device for the intended use.

Jim Moon Also, integration is often thought of as something that you do once: you get your network set up and make sure everything appears to be working. Instead, integration is really a continuum. That network is a dynamic thing and it’s changing all the time, whether it’s the movement of devices within the network, the number of devices, or the addition of yet another manufacturer’s device—a monitor, infusion pump, or whatever. So integration, performance monitoring, and looking at network statistics is going to be a continuous process.

Todd Cooper We have a moving target. The technology is changing all the time and consumers are changing. The application of risk management is very crucial, in not only the initial analysis for issues that need to be managed, but also for the monitoring and processing throughout the lifecycle of that network. Risk management is the process that helps us today and leads us to a better future in terms of safety, effectiveness, and security.

Don Witters Medical systems that use wireless or any other technology involve a paradigm of risk management that is not the same as that used in the IT world or the communications technology world. There are fundamental differences in what is needed and expected in medical systems versus other systems. Such risk management is typically done very well by medical device manufacturers, users, clinicians, and others who deal with patient care.

One of the big challenges I see is that open discussion on the real details—and reaching consensus on some of these details—is taking place very slowly in some areas, and perhaps not at all in others. We don’t have, for example, open and understandable information on the metrics that involve some of the wireless technologies. As Rick said, a small group of folks do under-
stand it and follow it closely. There is a general misunderstanding that wireless has a lot of capabilities it really doesn’t have, but it can be made to look that way by people who design and operate systems well. How well are those vendors’ systems scalable to these large efforts in the medical arena? And what these vendors want or need or intend to do is not so clear. So there are big challenges ahead.

**Mary Logan** What needs to happen next?

**Don Witters** Fortunately, there are groups discussing this actively and some real efforts being made to address challenges or at least to get a handle on what they are and make some framework by which they can be overcome. The IEC 80001 standards are a key building block for risk management in these kinds of systems.

**Bob Alberte** The radio frequency spectrum is crowded and that space within the hospital needs to be actively managed. Being successful in the wireless environment will depend on collaboration between medical device manufacturers and hospital IT personnel to ensure the key performance of the systems. IEC 80001 provides a framework for how that collaboration can be achieved and it is important to this discussion.

**Steve Baker** In many hospitals, the biomed and IT groups are distinct communities that don’t communicate well. In hospitals where they do communicate well, they have fewer problems. I’ve seen several hospitals where IT installs something and they don’t even know they’re stomping on top of a biomedical system until it turns it on and things blow up—patient monitoring and alarms are no longer able to be delivered, for example. Then they step back and go, “Oh my gosh. Look at this other network we didn’t even know existed.” If they were following IEC 80001 guidance, they would have a list of all known radiators in the hospital, allowing a risk-based approach to network changes and upgrades. Before installing a new system, they would look and say, “We have to consider this, this, and this.”

**Jim Moon** Healthcare facilities need to follow a solid ground-up network design process that addresses everything from equipment manufacturers and physical implementation, to the network plant, to the location of access points, etc. However, that kind of network design and management is often missing in healthcare facilities, probably because it’s not well understood.

**Rick Hampton** Similarly, the lack of communication between IT vendors and medical device manufacturers is still huge.

**Steve Baker** Yes, the interaction between network infrastructure equipment and multiple medical devices is definitely an issue. Components need to be tested to make sure they don’t have bad interactions. I’ve not tested hardware that randomly failed after it was released from one of these major vendors, but I have tested new firmware that, when we put our devices on it, failed to deliver information to the ultimate destination, despite working on a prior release of the firmware. The willingness of IT equipment manufacturers to work with medical device manufacturers to resolve issues has improved, and that’s important. If company X is not willing to work with medical device manufacturers to resolve issues related to safety and efficacy, it should not sell into hospitals.

**Don Witters** How risk is addressed by manufacturers of particular components, by people who integrate these components, and by people who deploy and maintain them is something that needs more open discussion. Consider Wi-Fi technologies, for example. People tend to see Wi-Fi as the only wireless option, but it was developed outside the medical or healthcare world. In some cases, it has great capabilities, but it’s constantly being improved. The newest Wi-Fi version has much greater capabilities, yet many devices and facilities utilize earlier versions because they’re less expensive and they work reasonably well in limited scope.

Healthcare is wide and diverse, with many stakeholders including the patient and clinician as well as the facilities. And now it’s going into private homes and other places where users are much less sophisticated than those in healthcare facilities.

The question is, are you addressing the risk for the intended use of that type of system in the environment where you expect it to be used? If this planning is done well, it can have great impact. If it’s done poorly, you can have issues.
Jim Moon We would all like to go wireless to achieve mobility, to simply unplug the cable and plug in the antenna and have it all work the same as it did over a hard-wired network. That’s just not realistic. We have to recognize that the wireless network is an imperfect communications network, and we need to address that in other layers of our system design and how we mitigate those wireless networking issues with other aspects of our system implementation.

Mary Logan What standards or regulatory/industry efforts are or should be underway to address the challenges you have just outlined?

Ed Cantwell You can consider wireless as a utility, similar to the electrical distribution system and increasingly, the voice over Internet protocol (VoIP) backbone. We know that we need this wireless “utility” and we know it is evolving. Those infrastructures as utilities came together by strong leadership across the ecosystem. It’s time to do that for wireless. At the West Wireless Health Institute, we’re going to try to solve this problem. Everybody stands to benefit if we do it right; everybody will suffer if it’s not done.

If we can come together as an industry and not shy away from addressing a definition of assurance for each type of network—each grade of service, each type of network, each particular frequency, each particular protocol in its environment of intended use—we should be able to address the risk and we should be able to architect infrastructures to reduce risk where it is possible and where it is important.

I’m optimistic. Wireless is going through the same problem that VoIP went through in hospitals. Where there’s a common VoIP backbone and it is treated as a utility, it’s very well designed and well managed. It’s very well controlled, as is electricity. That’s where we need to focus our time and money. We need to be responsible in making sure the delivery of wireless inside a premise is well thought out. If it is done correctly, there is a level of protection that almost transcends electricity.

Solving this problem is complex but achievable. And it’s almost nonsensical to think about introducing the next 1,000 wireless devices when you know you’re going into a crowded highway that is not very well built. We need to look at infrastructure first, then wisely deploy infrastructure so the risk stratification process is looked after device by device.

Don Witters I think the regulatory arena is building things in as cooperative and communicative a way as possible. First, we need to have a good handle on what all of these technologies mean in terms of a medical use. What is medical grade in terms of wireless? We don’t have much information about what the attributes of that need to be. Second, we need to understand what quality of service is needed for the range of uses and risks and still maintain safety. Third, we need a much better handle on what we describe as co-existence. So many wireless products are operating in the same frequency ranges and the number of people operating outside the medical arena in the same frequency ranges is growing exponentially. These products and medical devices need to coexist so that high-priority medical systems are able to function properly when they are needed.

And we need to have a better handle on security for wireless systems. Encryption is generally recommended in most of these situations, not only for device security but also for privacy. There needs to be an agreement on a level of security based on the risk itself. In homes, maybe that’s as simple as enabling the first level of security. In a nursing home or secondary care facility, maybe it needs to be better than that depending on what’s used. But some plan for those areas really needs to be developed.

News about the 80001 standards needs to get out to more wireless and IT folks. Before we move forward, the healthcare industry and especially hospitals need to understand there is no magic in these many wireless technologies. There are risks that must be identified, addressed, and mitigated. If we don’t know what those risks are and we don’t know how to mitigate them, we’ll never be able to build a safe system around them.

Rick Hampton News about the 80001 standards needs to get out to more wireless and IT folks. Before we move forward, the healthcare industry and especially hospitals need to understand there is no magic in these many wireless technologies. There are risks that must be identified, addressed, and mitigated. If we don’t know what those risks are and we don’t know how to mitigate them, we’ll never be able...
to build a safe system around them. We’ve got to begin addressing those risks before we can determine what constitutes a standard for medical grade systems. The healthcare and IT industries need to acknowledge these risks must be addressed and begin implementing risk-management activities as described by the 80001 standards.

**Jim Moon** The Wi-Fi Alliance is an industry organization that serves the interests of both the component and device manufacturers. As medical device manufacturers, we need to interface with that organization on a significant basis simply because it is one of the louder voices. If we don’t weigh in from the medical perspective, other industry segments will have a louder voice at the table when it comes to what direction they take.

**Rick Hampton** The Wi-Fi Alliance recently published a white paper on medical devices. This was an important step, and means that they are looking into these issues now. In the past they absolutely rejected any notion that they should be involved in medical devices. We need to work with the Wi-Fi Alliance and we need to get more people involved. The IEEE 802.11 group is another that could help. It’s going to take some concerted effort to get organizations like these involved.

**Bob Alberte** The IEC standard 60601-1-2 includes radio frequency (RF) immunity tests that help manufacturers determine the potential for interference between medical devices and RF-emitting devices. Monitoring devices undergo validation testing, which includes testing against this standard.

**Todd Cooper** IT, telecom, and medical device vendors need a place to do integration, interoperability, and coexistence testing. Currently medical device manufacturers are forced to do one-off testing, where a medical device vendor goes to a specific infrastructure company and tests their equipment on that infrastructure to get it to work. That’s great for the telecom company but very difficult for the medical device vendors.

**Don Witters** I think everybody here recognizes the tremendous possibilities with utilization of wireless technology in healthcare. And many of these technologies have already worked well. I can’t think of any group of people that isn’t touched by this kind of discussion or will be in the future. Stakeholders include virtually everybody. One of the biggest challenges and greatest opportunities is to work with all the stakeholders and engage them to develop these things that will push us into the next realm.

**References**

