What’s happening out there?

A special compilation of AAMI interoperability articles and resources
About This Compilation

AAMI has created this special compilation of resources to provide insight and practical guidance to the healthcare technology community. These articles—originally published in AAMI’s journal, magazine, and by AAMI’s Foundation—examine the major interoperability challenges in healthcare. We encourage you to read the publication and apply lessons to improve patient safety, share this document with your colleagues, and nudge other organizations to help address these important issues.

About AAMI

The Association for the Advancement of Medical Instrumentation (AAMI), a nonprofit organization founded in 1967, is a diverse alliance of nearly 7,000 members from around the world united by one critical mission—supporting the healthcare community in the development, management, and use of safe and effective medical technology.

AAMI serves as a convener of diverse groups of committed professionals with one common goal—improving patient outcomes. AAMI also produces expert and objective information on medical technology and related processes and issues. AAMI is not an advocacy organization and prides itself on the objectivity of its work.

Mention of any commercial product, process, or service by trade name, trademark, manufacturer, or otherwise in this publication does not constitute or imply an endorsement or recommendation by AAMI. The views and opinions of the authors do not state or reflect the opinion of AAMI.
Achieving Interoperability

Contents

3  Shatter-Proof Glass: From Cars to Healthcare

4  Achieving Interoperability: What’s Happening Out There?

14 All Systems Go: How System Engineering Can Improve Healthcare Technology

23 Wireless Ahead: Integrating Medical Devices into IT Networks

29 Step-by-Step Risk Management for Medical IT Networks

37 Safety Innovations: Best Practice Recommendations For Infusion Pump-Information Network Integration
AAMI Programs Making a Difference

**Standards**—AAMI is a leading source of consensus standards and guidelines to expedite and enhance the development, management, and use of healthcare technology. More than 100 AAMI technical committees and working groups write medical device standards, recommended practices, and technical information reports on issues ranging from sterilization to dialysis and clinical alarms to electromedical equipment. E-mail: standards@aami.org.

**Publications**—AAMI offers several complimentary publications to keep members up to date on standards and regulations, new technologies, policy developments, and guidance. Visit www.aami.org/publications.

**Books & CDs**—AAMI’s comprehensive and practical books and manuals cover a wide variety of important topics including sterilization, information technology, accreditation, human factors, healthcare technology management, quality systems, and certification. Visit www.aami.org/publications/books.

**AAMI’s Annual Conference & Expo**—It’s the premier conference for healthcare technology management—a three-day networking and learning experience that features the best and brightest speakers discussing key issues affecting patient safety and the healthcare technology management profession. To learn more, visit www.aami.org/ac.

**International Standards Conference**—The AAMI/FDA International Conference on Medical Device Standards and Regulation is a unique annual event bringing together industry and government leaders to explore the latest developments in international standards key to global market access and regulatory compliance. To learn more, visit www.aami.org/isc.

**Training Programs**—AAMI provides numerous face-to-face training programs, and online courses and webinars covering critical topics such as quality systems, sterilization, clinical engineering, design control, process and software validation, risk management, documents/records, statistics, purchasing controls, human factors, benchmarking, and IT issues. To learn more, visit www.aami.org/meetings.

**Certification**—AAMI provides leadership in public safety through the oversight of the International Certification Commission’s certification programs for biomedical equipment technicians (CBET), radiology equipment specialists (CRES), and laboratory equipment specialists (CLES). To learn more, visit www.aami.org/certification.

**Benchmarking**—AAMI offers two web-based benchmarking tools designed specifically to help healthcare technology management and sterile processing departments measure their practices, policies, and procedures against similar departments at other facilities. Visit www.aami.org/benchmarking.

**Healthcare Technology Safety Institute (HTSI)**—The AAMI Foundation’s HTSI is a new community of leaders focused on a common vision, “Healthcare technology will advance patient safety and will do no harm.” HTSI engages the healthcare community in multidisciplinary safety initiatives to strengthen the development, management, and use of healthcare technology for improved patient outcomes. To get involved, e-mail htsi@aami.org or visit www.aami.org/htsi.
For much of this year, a recurring theme in “what keeps me up at night” is the need for systems engineering in healthcare. At the core of this need is the rapidly growing dependency on and complexity of technology in healthcare, which has far surpassed the current organizational capacity of most hospitals to manage and prioritize emergent properties in order to ensure the safety of those systems. This chaotic complexity also puts enormous pressure on regulatory frameworks that were not designed with complex technology-oriented systems in mind.

In June, I had the opportunity to meet and hear a thoughtful keynote address at the INCOSE International Symposium, by Stephen Welby, deputy assistant secretary of defense. Welby is the first person to serve in a newly authorized (by Congress) senior engineering role in the DOD. His job is essentially to bring systems engineering expertise to DOD procurements. In the Q&A, Welby was asked what keeps him up at night. His answer: healthcare. Five percent of the entire cost of healthcare in the United States is incurred by the DOD and VA. Engineers can help reduce the cost and increase the value of healthcare, if we give them a chance to do so.

I spent the rest of this same day participating in a panel with Welby and a group of senior systems engineering leaders from many domains: aerospace, transportation, satellite communications, and the like. These giants have moved through many of the same technology challenges that healthcare faces today. The major difference: these other industries are mature in using systems engineers, principles, and thinking as a foundational tool.

Here’s a simple example. The windshield on our cars today is shatter proof. That windshield was designed using systems engineering principles, and is now a key part of the overall safety system that surrounds and thus protects humans in a crash. Shatter-proof glass is an example of a systems-based shift in the culture of automotive safety design, which has moved from a rescue model (how quickly can we pull an injured person out of a smashed car before it explodes) to a planned model that looks at the windshield not as a screen for bugs but as a part of a safety system.

Shatter-proof glass may or may not have uses in healthcare. The systems engineering principles and leadership that led to this cultural shift in automobile design are greatly needed in healthcare.

Healthcare delivery organizations in the United States spend billions of dollars annually on rescuing our human bodies that betray us with a multitude of traumas, diseases, and conditions. The rescue culture is deeply embedded in healthcare, where committed individuals drop and do everything to save a human life.

How many dollars are being invested in improving healthcare through planned systems engineering, as opposed to patient rescuing?

In the past year, the need for this problem to be addressed with greater intention in healthcare has been evident in the AAMI/FDA Interoperability Summit, the Wireless Workshop and subsequent task force discussions and articles, and the cover story of the March/April issue of BI&T.

Most hospitals do not have human factors, systems, process safety, or clinical engineers on staff, and complex “technology” challenges are increasingly going to IT to manage and solve because of the increasing emphasis on the EHR and related technologies in the IT domain. Systems engineering is not IT. It’s a much more holistic and comprehensive approach to engineering, and that’s why it’s needed.

Medical device industries also need more systems engineers, and individuals who come to medical device companies from other high reliability industries are a special breed. We need more of them across healthcare.

When giving me advice, one of my senior staff is fond of saying, “If I were king of the forest.” To borrow his phrase, “If I were king of the forest” as the CEO of a medical device company or healthcare delivery system, I would follow the rare wisdom of Congress and hire a systems engineer like Stephen Welby. In my forest, that individual would serve in the role of chief technology officer and would be part of the senior management team, reporting up to the CEO or CFO. The ROI would not be in the next quarter, and might not be in the next year, but the ROI is definitely there.

Healthcare needs less rescue and more multidisciplinary planning, design, and development. There’s an Rx for that: systems engineering.
Interoperability is a popular word in the world of medical devices, and many believe it is the answer to some of healthcare’s thorniest problems. This article takes a close look at what three healthcare facilities are doing today with one very important piece of the interoperability puzzle: the integration of device data into electronic medical records (EMRs). Their stories make it clear that what seemed impossible only a few years ago is now becoming commonplace.
The current EMR push is in response to one very important development: The federal government has promised $19 billion to hospitals and physicians who can demonstrate “meaningful use” of EMRs through the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009. Feeding device data directly into EMRs is seen by most as a key part of this effort.

As hospitals rush to achieve meaningful use, clinicians are starting to see real benefits from the faster availability of more accurate data in medical records. Yet the path to full interoperability is not smooth. Those pushing the boundaries of what’s possible often find themselves stuck in a quagmire of poorly defined standards, incompatible systems, infrastructure problems, and vendors who sometimes spend more time pointing fingers at other vendors than they spend resolving problems. As projects flounder, no arbitrator is available to resolve disputes. And even more significantly, very real patient safety concerns are raised about the foundations of interoperability.

How can healthcare organizations achieve the promise of interoperability and avoid the pitfalls? These case studies offer some important hints:

- **Start small.** Lessons learned from pilot projects of limited scope will help you establish relationships, learn about your systems, and solve foundational problems before moving to larger, more complicated projects.
- **Involve both clinical engineering and information technology professionals.** Both skill sets are essential to success.
- **Use quality systems and risk management tools to evaluate safety issues caused by building systems of systems.**
- **Test, test, and test some more—before, during, and after project implementation.**
- **Consider pre-existing vendor relationships carefully.** Particular EMR vendors have different relationships with medical device vendors; the effectiveness of those relationships will have a huge impact on the success of your project.

Above all, these case studies demonstrate that the benefits of integrating device data into EMRs for clinician workflow and patient safety are real, but so are the risks.

### CASE STUDY 1

**Good Planning Leads to Smooth Integration of Bedside Monitor Data**

The story of device integration at the two-hospital, 900-bed Gainesville campus of Shands HealthCare at the University of Florida is a smooth one so far. Within seven months, the clinical engineering (CE) and information systems (IS) departments successfully integrated data from 560 bedside monitors into a new electronic medical record system at minimal cost and with remarkably few problems. Their secret? Good technology choices made years before.

As hospitals rush to achieve meaningful use, clinicians are starting to see real benefits from the faster availability of more accurate data in medical records. Yet the path to full interoperability is not smooth.

The top half of this diagram depicts the patient monitoring interfaces for the HL7 gateways at the Gainesville campus of Shands at the University of Florida. The bottom half shows how the data reaches either Epic or Centricity. The thick black horizontal line and the one thick vertical line represent the hospital data network.

---

**About the Author**

Jill Schlabig Williams served as project manager for the AAMI Foundation’s Healthcare Technology Safety Institute. E-mail: jwilliams@aami.org
underway, they are already looking to bigger challenges ahead.

Bedside monitor data integration efforts at the campus formally began in 2010, but the foundation for the effort was laid several years earlier. In 2002, Craig Bakuzonis, director of the 21-person CE department of the Gainesville campus, took part in an effort to build a new pediatric intensive care unit. Both physicians and nurses involved in the project wanted to look at moving the facility toward electronic records. “We were planning a new intensive care unit and wanted connectivity options,” he says. “At that time, connectivity was viewed as something coming near-term. We did some research and confirmed with our vendors that HL7 was the standard to use for data interchange, and we used that standard to guide our technology purchases.”

Health Level Seven, or HL7, is a framework and set of standards for the exchange, integration, sharing, and retrieval of electronic health information. It permits medical devices to send data to EMRs.

“The IS department and I saw that at some point the hospital would want to do electronic documentation of vital signs data from bedside monitors,” says Bakuzonis. They chose to purchase the Philips Intellivue architecture and also purchased the related gateways as an option up front. These gateways collect and store data from a group of monitors and allow forwarding of that data to EMRs.

“Nurses have to understand that numbering scheme, as they are responsible for associating the patient with the monitor in the system,” says Bakuzonis. “As we grow, the pieces were in place to integrate the monitor system data directly into the EMR,” says Bakuzonis. “We did not have to back-fit connectivity to any legacy monitors.”

The Project
In November 2009, Epic was selected as the EMR vendor of choice. Installation began in January 2010, and by May they went live with bedside monitor integration.

Bakuzonis was able to draw from some earlier experience with data integration for this project. He had been involved with installing electronic documentation in an anesthesia department in 2005 when the hospital opened a new outpatient surgery center. “They wanted the documentation to be entirely electronic, and decided to use GE Centricity as their preferred intraoperative anesthesia system,” he says. “It’s still in use today, but that may change eventually.”

As a first step for the bedside monitor integration, the IS and CE departments formed a device integration subcommittee comprised of experts from each group. This team worked to gather data on bedside device models and locations, plan data export, and map parameters to the Epic system. IS took the lead on interfacing, applications, and parameter mapping. Some cabling infrastructure upgrades were required. The CE team worked closely with Philips to understand the gateway system, assign IP addresses, configure central stations for HL7 export, and rename monitors.

Renaming monitors was one of the first challenges they faced. Each bedside monitor would need a unique “name” so that patients could be associated with that monitor, allowing data to flow from the monitor into the correct patient record in the EMR.

The price per bed was very reasonable. For a 24-bed ICU, connectivity costs totaled less than one percent,” says Bakuzonis. “I was very comfortable that we would see a big return on a small investment.”

For the next several years, Bakuzonis and his team gradually replaced earlier-generation Philips monitors with the integration-ready newer models. By 2010, their entire inventory had been replaced. “By the time our EMR vendor was chosen, all of

Lessons Learned at Shands
Craig Bakuzonis says his CE department learned many lessons during the project, including:

- Keep detailed information about configurations readily available.
- Work with IS help desk and interface engineers to develop a problem resolution plan.
- Adopt a formal change management process. CE has discovered that they have less flexibility now that their Philips system is no longer a stand-alone network and that they have to coordinate work with IS. They are now adopting the IS model for change management.
- Develop a process for downtime procedures (planned and unplanned).

** Renaming monitors was one of the first challenges they faced. Each bedside monitor would need a unique “name” so that patients could be associated with that monitor, allowing data to flow from the monitor into the correct patient record in the EMR. **
that 6-digit limit may need to be modified.”

Configuring the Philips export engine was also a challenge. “It’s not an ideal export engine, and it took time to figure out the system,” says Bakuzonis. He worked with the vendor, read the documentation, worked with IS, and relied on his previous experience with the anesthesia information system to figure out how to do it. He and Philips trained six CE staff members. “We handled the programming and configuring of the Philips gateways, as we were viewed as the people who knew the system best.” Monitoring was also the CE group’s responsibility. IS took over at the point where data exited the gateway system.

Another challenge involved choosing which parameters to map into the Epic system out of the 100 or so that are available from the Philips monitors. That piece of the project was handled by IS. “Parameter mapping was painful,” says Pedro Hernandez, an application support analyst with the IS group. “We had to go through a process of trying to get everyone to agree and to align nursing practices.” Nursing leadership had to standardize the use of parameter labels and trim back the number of parameters that should be mapped from the hundreds that were available. “It took about two months to do the data mapping,” says Hernandez.

In the process, they discovered a problematic limitation: a 30-parameter limit with the Philips HL7 export engine. This affects data to both Epic and the GE Centricity system. “We don’t like those restrictions and would like to be able to document more parameters,” says Bakuzonis. “For complex open heart procedures or neurosurgery, we find that we’re exceeding that parameter count. For now we’re making an attempt to get the most important 30 parameters, but we would like to eliminate the problem. We’re actively working with Philips to expand that 30-parameter limit.”

Extensive testing was conducted on the system prior to go-live. “We had a good comfort level that data labels were correct,” says Bakuzonis. “IS ran tests on random bedsides to confirm connectivity. Go-live was the ultimate test, and we were able to confirm that we had successfully matched patient data between systems.”

“Parameter mapping was painful. We had to go through a process of trying to get everyone to agree and to align nursing practices.”—Pedro Hernandez, Shands HealthCare

Bakuzonis reports that the go-live was relatively smooth. “Everyone had to remember their training,” he said. “There were a few hiccups, but within 48 hours it was clear that the system would work.” Once the system was running, he says, not a lot of support was needed.

Results

Today, Phase I of the project is complete. All 560 monitored beds feed their respective systems every day. The seven-month implementation required intense cooperation between IS and CE, and set the stage for the next phases of the planned five-year project. (See the sidebar on this page for more information on the next phases.)

Most importantly, they achieved their goal of fewer transcription errors and timelier entry of patient vital signs data. “People rely heavily on the monitors documenting directly into Epic,” says Bakuzonis. “It saves clinicians a lot of time. It’s become a huge tool for the nurses, and we hear complaints quickly when it goes down.”

Future challenges for the team at Shands Gainesville include improving network management ability. “We realize that now, entire systems are used for data export and that the entire system needs to be reliable,” says Bakuzonis. He is also looking ahead to networking stand-alone devices like ventilators, cardiac output monitors and other legacy devices and installing wireless infusion pumps.

All in all, the group at Shands Gainesville is very happy with the success of the project. “Integration happened because we made a plan to have integration options,” says Bakuzonis. “Our initial plan with Epic was that if devices had the opportunity to connect to Epic without significant additional cost, we would connect them. There was no big study, no hospital-wide effort. We all knew the potential and took the next, natural step to connect devices.”

### EMR Implementation Project Phases at Shands

<table>
<thead>
<tr>
<th>Phase</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (complete)</td>
<td>Epic electronic chart for all inpatient care areas (acute, ICU, labor and delivery), inpatient pharmacy, CPOE, HIRM documentation tracking</td>
</tr>
<tr>
<td>2 (ongoing)</td>
<td>Scheduling, ADT, billing/coding, outpatient clinic charting, patient customer information access</td>
</tr>
<tr>
<td>3 (2012)</td>
<td>Radiology and oncology ancillary departments</td>
</tr>
<tr>
<td>4 (2013)</td>
<td>Home health, cardiology, transplant, and OR/anesthesia ancillary departments</td>
</tr>
<tr>
<td>5 (2014)</td>
<td>Lab and outpatient pharmacy ancillary departments</td>
</tr>
</tbody>
</table>

There may be additional device integration projects with the outpatient clinics and the other ancillary departments, says Craig Bakuzonis, director of the Clinical Engineering Department at Shands.

### Related Story

See the “IT World” column on page 64 for a look at how safety concerns can limit functionality when it comes to the integration of patient data.
Using Integrated Data to Improve Patient Care

Indiana University Health (IUH) started its journey to device integration in 2001 when it partnered with Cerner to develop an EMR that was completely integrated. “We wanted all patient information in one medical record,” says R. Renee Johnson, RN, MBA, the IT clinical project manager and critical care nurse that assists with the integration efforts at the 20+ hospital system based in Indianapolis.

The health system was responding to patient safety concerns raised in To Err is Human, the landmark 1999 Institute of Medicine Report which estimated that between 48,000 and 99,000 patients die each year due to preventable medical errors. There were other problems as well: “We were seeing fewer physicians and nurses, rapid population growth, and financial con- straints,” says Johnson.

Rather than focusing on time savings, Johnson tries to teach a new workflow. She says, “Acknowledge that it’s not easy at first, but emphasize that it will get easier. Highlight the benefits to nurses: it allows them to care for patients first, then they can catch up on missed vital signs. Data are more accurate. Paperwork doesn’t get lost. There is more continuity of care. Things are less likely to be misread since we’re not relying on handwriting. They will see improvements in care because of timeliness, wider availability of data.”

“Keep in mind that no one is eager for change,” she adds. “Try your best to ease and validate their fears up front. The more training you can offer, the better.” To entice nurses to attend training, Johnson has offered food and candy at training sessions and even prizes, along with daily newsletters to staff during go-live to keep them informed of project status.

A NURSE’S PERSPECTIVE

R. Renee Johnson’s career path from critical care nurse to IT project manager at IUH has given her some useful insights on how to introduce these new integrated technologies to clinicians. “When we first introduced these technologies, the message was that technology would speed things up and make documenting easier. That is not necessarily true. Things certainly are not easier in the beginning or in a critical care environment where data have to be captured frequently. It’s only easier in the long run, once you get used to it. Nurses always have an initial transition period.”

With most integrated systems, data flows continually to a gateway server which collects the data and stores it, often for 12 hours before it is deleted. When a nurse wants to record vital signs data for a patient, she must first go into an association screen and associate a location identifier and the devices with the patient. The data are then associated with the patient, but still not recorded in the chart. The nurse picks the data to save and validate, and that validated data then flows into the patient’s record.
IUH turned to technology as one answer. “Our goal was to use technology to leverage the experience of our doctors and nurses, decrease the length of stay, decrease variations in practice, and implement best practices,” she says. “We hoped that integrating device data into the EMR would allow us to reduce documentation errors, increase patient safety, decrease communication errors, increase quality, improve workflows, reduce redundancy, and fully integrate the patient records into one place.”

**Device-EMR Integration Key**
To improve safety, the health system developed a Virtual Care Center, an in-patient remote monitoring center and tele-ICU launched in 2005 that monitors 305 beds at four hospitals. The center was designed as a second-layer safety and quality net, and offers real-time vital signs, audio and visual capabilities, alerts and trends, call buttons in rooms, and cameras. “It allows our intensivists to go home after hours because physicians in the bunker help monitor their patients. Also, it gives nurses someone to call for a second opinion.”

Device data integration was seen as key to the ongoing success of the center. In 2005, the first biomedical device integration (BMDI) team was formed to find a way to feed data directly from devices into the EMR and to the virtual center. In 2007, the team tried to go live with nursing clinical documentation, but encountered multiple performance and adoption issues. The team tried again in 2008 and achieved success at a downtown hospital. As of September 2011, all facilities are live feeding device data in the Cerner Millennium EMR system.

**Multipronged Integration Effort**
Unlike Shands in Gainesville, IUH has multiple devices connecting to the EMR in multiple ways. Both stand-alone and networked devices feed into the EMR. “We connect using a variety of different methods,” says Jeff Lane, the team leader for BMDI services. They have gateway feeds that come from vendor-specific device networks. They also use a third-party, (device vendor-neutral) gateway, and Cerner’s new iBus product (Cerner’s version of a gateway) to connect devices that do not use vendor gateways such as anesthesia machines, ventilators, cardiac output monitors, and others. A team of four BMDI employees support day-to-day operations and all projects.

The process of connecting all of those devices was anything but smooth, says Lane: “Where devices are networked, we normally get an HL7 feed from a gateway. For legacy devices, we had to get upgrades, purchase gateways, and/or purchase servers to connect them all together.”

“We hoped that integrating device data into the EMR would allow us to reduce documentation errors, increase patient safety, decrease communication errors, increase quality, improve workflows, reduce redundancy, and fully integrate the patient records into one place.”
—R. Renee Johnson, Indiana University Health

“The installation process varies depending on the equipment,” says Lane. For monitors, the vendor installs the system while the BMDI group advises on naming conventions, tests data flow, and sets up equipment. The third-party, device vendor-neutral gateway or iBus products help them connect legacy devices. Lane reports that the iBus system is newer and that in some instances they have
Lessons Learned at IUH

- Develop a partnership between IS and biomed. When integrating devices, the two areas have a lot to offer each other. Both need to understand what roles they need to play.

- Remember that nurses need to be able to use all of this equipment, the devices as well as the interface and the EMR. For example, consider placement of monitors; if the connectors are too high, nurses can’t ensure good connections to get data to flow properly.

- CE needs to understand implications of new device purchases on connectivity. Standardize on just a few device vendors; consider the existing infrastructure.

- Assess the clinicians’ culture — how well will a particular unit adapt to automation? Keep in mind that the right leadership is needed to help drive the effort forward.

- When building new facilities, understand that device installation has to occur much earlier in the process in order to test device interfaces.

- Name devices with something that makes sense so that clinicians can identify the device and the room and associate it properly with the patient.

chosen to stay with the third-party vendor-neutral solution to maintain desired capabilities.

Lane’s BMDI team works closely with both the IS department’s desktop service group and with the biomed department. “We’ve had a close relationship with biomed since we implemented device data integration in the first facility, and I’m often in close contact with them,” says Lane. “We split responsibilities for this equipment: biomed handles clinical equipment, and BMDI takes care of items from the serial port out. But still, there’s a gray area there. Where should clinicians report problems first?”

Cross training and cross staffing have helped cooperation between the two groups. A clinical engineer joined the BMDI team; biomed has been trained on cabling, and IS staff is cross-trained to troubleshoot equipment. “We maintain separate areas of expertise, but we often attack issues as a team,” says Lane. “It is critical to build a relationship with biomed right from the start.”

The health system has faced a long list of challenges in its integration efforts, including funding; integrating disparate devices and networking legacy equipment; solving patient association problems; ensuring that time stamps are correct; mapping parameters and developing a data dictionary; changing culture and encouraging adoption; keeping up with technology changes; lack of vendor-neutral hardware; latency of data; too much data and not enough information; and infrastructure problems. The biggest items on their wish list are medical devices with native HL7 outputs so they can hook devices directly to the network.

Integration Benefits Huge

While the implementation process may be rocky, the benefits of a successful implementation are huge. “There are many clinicians in the workplace now who have only documented electronically so when the system goes down, they have to revert to paper which can be a hardship,” says Johnson.

“We have found that as we add integrated technologies to new areas of hospitals, BMDI seems to be a deal breaker. If they can’t use BMDI, they don’t want to perform any upgrades,” says Lane. “Clinicians have come to rely on that data being available. It also most seems to cause them hardships when it is down for any reason. BMDI is a product that just seems to work. It is usually very reliable. When it breaks, it’s usually because of a larger problem.”

Despite its progress at automating patient records, IUH is a hybrid, still using some paper records. Implementation efforts are ongoing. And looking ahead, the health system is considering adding devices that would assist with tracking, perhaps badge scanners that identify staff when entering patient rooms. They’re also looking at infusion management or integrated smart pumps with bidirectional interfaces, alarms development, contextual passing, alerts maturation, and decision support.

“The sky’s the limit,” says Johnson. She is currently working on a project to create a dashboard screen of the most critical information. “We’re in a data-rich, information-poor environment,” says Johnson. “We have lots of data, but it’s not always where you need it. We’re looking at ways to improve that.”

CASE STUDY 3

Device Integration Promise and Pitfalls

Children’s National Medical Center, a 306-bed freestanding children’s hospital located in Washington, DC, is fortunate to have excellent resources at its disposal, with access to some of the leading medical and technology experts in the country. Its financial strength allows it to apply the latest cutting-edge technologies to improve care and save children’s lives.

The team at Children’s was successful early on at integrating device data into its EMR and achieving significant improvements in patient care as a result. Yet, as they have moved beyond the early stages of implementation and into more complex projects, the integration experts at Children’s have run into several dead ends that have resulted in wasted money, underutilized systems, and
untapped potential. The team is learning first-hand about the brave new world of device integration where systems conflict, software upgrades destroy data flow, and vendors talk rather than solve problems.

The Promise of Integration

In 2004, Children’s began looking at ways to use technology to improve patient safety. “We decided that the biggest bang for the buck was in avoiding medication errors,” says Brian Jacobs, MD, the hospital’s chief medical information officer. They began looking at the benefits of EMRs in terms of computerized physician order entry (CPOE), nurse documentation, and digital radiology. “The literature and our experience suggested the greatest risk of medication errors is in the prescribing process due to illegible or incomplete orders, no signatures, and pharmacists having to speak with clinicians to clarify orders.”

So, in 2005, the hospital started off with CPOE and electronic medication administration records (eMAR) systems. Around the same time, the hospital chose to move forward with Cerner as its EMR, and committed to partner with them on using Cerner I-View as the intensive care charting portion for vital signs. By 2008, they began roll-out of a full electronic medical record system, including integration of device data into the EMR. “Our goal was to feed data from four units: the pediatric, neonatal, and cardiac intensive care units (ICUs), and the heart-kidney unit,” says Jeff Hooper, the clinical engineering director for Children’s.

Hooper and his colleagues in the IT Department began to form a team around the implementation of the EMR. One clinical engineer, Virginia Amendola, moved into the IT Department for the implementation process and now manages ongoing integration projects from within the CE Department. They encountered and overcame several obstacles in the implementation process, including learning the system, choosing parameters, mapping the data, and a testing process that Amendola describes as “physically and mentally draining.” But by May 2008, the project was up and running to rave reviews.

LaTasha Burns, a nurse and clinical informatics manager, says that the project went well. “It was probably one of our biggest wins,” she says. “Clinicians appreciate anything that can save them time, and we can build on this foundation.”

Device interoperability is important, and efficiency and accuracy of data flow is especially important in a pediatric environment. Neonatal, pediatric, and cardiac intensive care units (ICUs) include a lot of very sick kids, with intense data flow. We can have up to 11 infusions going on one patient.

Before data integration, nurses or respiratory therapists were going in every 15 minutes and hand charting several parameters on a four-page spreadsheet. These handwritten sheets could be illegible and often included transcription/math errors. At the end of the day, the nurses would enter a long spreadsheet of data into the computer for each patient.

As a critical care doc, I would come in at the change of shift and want to know what’s going on with my patients. Under the old system, the data were not available until the nurse finished charting. Often, I’d be waiting for data that a nurse hadn’t even had a chance to add up.

Now, I can pull up complete, legible information quickly and conveniently without having to wait for the signout process. Integration eliminates all of data entry and waiting. Instead, the nurse selects a column which autopopulates, the nurse validates that the data is correct, and it feeds into the EMR where everyone who needs it can see it. There is a huge efficiency gain and accuracy gain.
New Challenges

The success of the initial project helped the team—and the clinicians—recognize the value in integrating device data into the EMR. So they wanted more: integration of two types of ventilators and also cerebral oxygen monitors. And alarm integration. And infusion pumps. And with every new implementation, new challenges had to be faced.

In one case, the team upgraded to a new system that didn’t work and had to backtrack to the original system just before go-live. They had initially integrated the ventilator and cerebral oxygen monitor data by using a Philips ViewLink device. When they wanted to bypass the ViewLink device in order to free it up for alarm management and data storage, they purchased a new CareAware device interface from Cerner. In testing, they noticed that they were getting fewer parameters through the CareAware device feed.

“We discovered that we had to write a separate driver to access all of the data we had been getting previously. We just couldn’t do it at that point, and had to go back to the ViewLink device. We spent the extra money, bought extra devices, and were not getting even as much data as we were getting before,” Amendola says.

In another case, the lack of standards and interoperability in device data feeds is limiting their capabilities. Brian Jacobs came up with the idea of detecting ventilator malfunctions and adverse events through the EMR. “When there’s a problem with a device being used on a patient and it has to be changed out, the device ID changes. That would indicate that a ventilator has malfunctioned,” he says. “We wanted to use the act of changing a ventilator ID as a proxy for ‘an adverse event may have occurred.’”

While that sounds easy, it turns out that ventilators do not send out a device ID with their data feed, meaning that no device ID change would be documented in the EMR. To get around the problem, they’ve asked nurses to enter the six-digit biomed device tracking number into the system, which involved a training effort, policy changes, and action on the part of the nurses.

Amendola tells of a software upgrade to the CICU monitors that knocked out certain parameters that had previously been flowing...
into the EMR. “The software upgrade tweaked BMDI codes for only a few parameters. The nurses noticed the lost parameters and complained. We discovered the vendor had implemented new codes with its software upgrade. To solve the problem, we took all monitors back to the same software revision that worked. Now, we must downgrade all devices to Revision F; we are missing Revisions G and H. And we discovered that the HL7 coding doesn’t come from the database server, but rather is generated in the monitor itself.”

Hooper says that they’d like to integrate their 800 infusion pumps into the EMR but can’t seem to do it without buying a $2 million wireless upgrade from the manufacturer. “Specifically, the syringe pumps we use no longer have an ‘output’ or RS232 port. Vendors seem to be moving in the direction of a server-based or networked approach, which is difficult since it requires you to purchase the networked solution and in this case a bedside connection, which leads to involvement of another vendor and more hardware to connect, further relationship and connection issues, and higher costs. It’s led to months of high-level meetings between the device vendor and the EMR company with no resolution.”

“There are some devices with only one or two parameters that we’d love to integrate but it’s just not worth spending a year and a half to do it,” he says. “We’ve therefore found ourselves unwilling to integrate new devices. That’s a long road for only one or two devices; we hope it becomes easier.”

Jacobs agrees. “Budget is less an issue in resolving problems, and it’s more a problem of the time required. We need to dedicate a team of biomed staff, IT staff, vendors, and Cerner to resolve every problem.”

In some cases, the medical device vendors and the EMR companies find themselves in competition. Jacobs offers an example: “One device vendor wants a robust reporting function, but the EMR has that already. Therefore, they compete over who will set standards for interoperability. We need to get developers to work together. These problems get into complex intellectual property issues, and can take months to resolve.”

Other problems they’ve encountered include unavailability of transport data and inability to send waveforms to the EMR. Plus, the hospital’s status as a pediatric facility creates challenging issues, as certain parameters unique to children are not even included in the EMRs. “This issue is unique to children’s hospitals and the vendors have not integrated those parameters as often because the need is not as great across the board,” says Hooper. As a result, Burns says, “We have to tweak the values for the pediatric population, and do more customization for pediatrics.”

Hooper and his colleges at Children’s would like to see uniform device IDs as part of the data flow for all devices; an automated patient/provider/location association; better time stamps; and data feeds available from all devices. “The goal is plug-and-play,” says Hooper.

Lessons Learned at Children’s National Medical Center

- The choice of an EMR system, once in place, drives everything. It is a significant long-term relationship. Choose wisely.
- A hospital needs to make sure there is a match between their EMR vendor and medical devices vendors. It is important that the two are aligned in their vision of interoperability.
- Do site visits with both vendors to see that the system works. Device vendors and EMR vendors are in various stages of their relationship; do your homework around that before committing to a purchase.
- Don’t just buy and implement new systems; think about the kind of value you want to derive from these investments and the metrics you’re trying to achieve up front.
- Test things before you make purchases, using exactly the same setup you plan to use live. Even if you have great relations with your vendor, you will not be able to understand the full capabilities without testing.
Achieving Interoperability

ALL SYSTEMS GO
How Systems Engineering Can Improve Healthcare Technology

By education and training, clinical engineers and other healthcare technology management (HTM) professionals are problem solvers. But today’s problems are markedly different than they were in the past—a trend that is accelerating as information technology (IT) becomes increasingly complex, connected, and crucial in healthcare. Tried and true tools and protocols for managing stand-alone equipment are proving insufficient for dealing with systems issues.

Right now, most healthcare technology managers inhabit an in-between world—one that straddles the “break–fix” mentality of the past and the systems thinking that experts believe is the future for improving patient safety and clinical practices.

“Over the past 10 years, my job as a clinical engineering director has changed from managing the majority of medical systems as stand-alone devices or isolated systems to, today, these same systems are either integrated or in the process of integration with other systems,” says Gregory Herr, director of clinical engineering at the Christ Hospital Health Network in Cincinnati, OH.

Donald Armstrong, a certified biomedical equipment technician with GE Healthcare, sees “a huge difference” in his responsibilities because of the growing systems dynamic. “We spend a lot more time these days tracking where the failure lies, instead of just fixing the immediate problem,” he says.

Pat Baird, an engineering director with Baxter Healthcare Corporation, sees real value in embracing systems thinking in healthcare. “The motivation that I have for bringing more systems theory to the health-

About the Author

Martha Vockley
is principal of VockleyLang, LLC, a communications and marketing firm based in Reston, VA. E-mail: rmv@cox.net

“Big whirls have little whirls,
That feed on their velocity;
And little whirls have lesser whirls,
And so on to viscosity.”
— Lewis Fry Richardson, English mathematician, physicist, meteorologist, psychologist, and pacifist
The care environment is that I see the people constantly reinventing the wheel in healthcare. Many of the challenges in healthcare are the same challenges other industries have faced decades ago. Healthcare needs to catch up and I think that “systems thinking” could help speed the process.”

### Understanding the Abstract

Getting to the practical side of systems thinking in healthcare first requires a journey through abstraction, because a system is “a whole bunch of levels of abstraction,” in the words of Lane Desborough, a product strategist with Medtronic.

Participants at the 2012 AAMI-FDA Interoperability Summit emphasized that people are an integral part of any system, because people interact with technology. Summit participants urged the use of the term “sociotechnical” to describe—and guide the design and life cycle of—systems in healthcare.

Recently, the phrase “system of systems” has been in vogue, and yes, there’s an acronym for that: SoS. Purists say that term is meaningless, however, and that “system” suffices and says it all.

Regardless of the terminology, the interaction of individual components is the key differentiator for true systems, or systems of systems, in healthcare technology, according to Ken Maddock, vice president of facility support services at Baylor Health Care System. “We have had networked medical devices tied to a back-end database for years,” he says. As an example, he cited electrocardiogram (ECG or EKG) systems. “You’d send an EKG cart out, and you’d run a 12-lead EKG on a patient. And you were able to hook those up to a network and download the studies. The devices connected, but they didn’t really interact.

“Most people are considering the device and the backend database to be a system of systems now,” Maddock adds. “A lot of people are confusing just connecting devices to a network and feeding data into an electronic health record [EHR] to be a system of systems. Even with the EHR, that is still basically one-way communications. To me the real system of systems is when you have live or close-to-live communication back and forth that impacts the setup of the device and the way the device interacts in some way with others.”

### What’s a System?

- “A system is built from a group of parts, whose combined interactions produce a behavior that no one part alone can produce.”
  — John Thomas, president, International Council of Systems Engineering

- “A system does something different than its constituent parts taken individually. It exhibits some property that the individual subcomponents don’t. So, for instance, flight is a system property of an aircraft. It’s only when you assemble the constituent parts—an engine, the wings, and the pilot together into a system—that this emergent property, or system property, of flight takes place.”
  — Lane Desborough, product strategist, Medtronic

- “A system is variously defined as ‘a group of interacting, interrelated, or interdependent elements forming a complex whole.’”
  — Raymond Zambuto, president, Clinical Engineering Concepts, LLC

Rick Schrenker, systems engineering manager with the Department of Biomedical Engineering at Massachusetts General Hospital, says systems share these concepts:

**Synergy**: The whole is greater than the sum of the parts.

**Emergence**: Value-added properties and capabilities of a system emerge only when the components are intentionally integrated (unless you want to rely on natural selection and evolutionary time scales).

**Boundary**: Systems are bounded. The properties and capabilities that add value are delivered across the boundary to a recipient. Similarly, a system is a recipient of information, goods, energy, and so on from outside its boundary that it uses to create that which it delivers.

A “system of systems” can be described as a group of interacting, interrelated, or interdependent systems forming a system. A hospital is obviously a system of systems—operating room, emergency room, nursing units, materials management, and so on. Ditto a regional healthcare delivery organization. At some point you extend the boundaries to include payers, including insurers and government agencies.
The challenge of any system is that desired behaviors, emergent properties, and interactions can go awry. In short, there are often unintended consequences.

The patient. It’s not just a dumb device anymore. It’s a device that knows who you are and is going to customize what it is doing based on who you are and what your condition is. The device has context.”

For Maddock, the use of infusion pumps provides a good way to understand how well designed and functioning systems can turn “dumb devices” into smart ones. In most applications, networks push out periodic drug library updates to infusion pumps—a one-way communication. For the few healthcare delivery organizations that are using systems to apply the “five rights” of drug administration (right patient, right drug, right dose, right route, right time), many connected systems interact back and forth to make that possible.

When a broad system is designed with an intended behavior such as the five rights built into it, it can contribute to improved patient care and clinical practices. Consider the care of a patient in a critical care unit. Baird sees three systems at work: The treatment for that patient involves a system of devices that are delivering drugs; another system of monitors that keeps tabs on the patient’s condition; and an EHR system to handle the patient’s medical history.

“If there’s a sudden change in the patient’s vitals, the nurse might need to refer to the medical records to check for allergic reactions or other complicating medical conditions before deciding on what changes need to be made to the drugs being delivered. So the clinician actually is working with three different systems every day, even with this simple example.”

The challenge of any system is that desired behaviors, emergent properties, and interactions can go awry. In short, there are often unintended consequences.

“The reason why this word ‘emergent’ is so attractive to me is that oftentimes the system properties don’t emerge until the system emerges,” Desborough adds. “In fact, by definition, an infusion pump sitting in a warehouse somewhere is doing no harm nor good until it’s purchased by a hospital and brought into a particular clinical setting and attached to a certain patient with a certain drug being infused through it. It does nothing until it’s part of a broader system.”

David Stiles, CBET and director of biomedical engineering and central equipment services at Long Beach (CA) Memorial Medical Center, has first-hand experience with system-propelled emergent properties and unintended consequences. “An example of our new challenges is the process of drug library revisions on our infusion devices that rely on quick broadcast to nursing, pharmacy, and information systems,” he says. “This new ‘system’ may not react or implement as designed—and this requires quick and unscheduled intervention.”

The Role of Systems Engineering

“Watch the little things; a small leak will sink a great ship.”

— Benjamin Franklin

Desired behaviors such as patient safety and clinical decision support could emerge from medical technology and health IT systems. But experts say these kinds of behaviors are unlikely to emerge unless systems engineering principles and tools are applied, beginning in the design stage, to produce them. Worse, failure to attend to potential unintended consequences could compromise patient safety—a prospect that is increasing as more components and systems are connected.

That's where systems engineering will be valuable. “In my mind, systems engineering is as simple as balancing what you're trying to achieve versus what are the potential unintended consequences of connecting all of these things together,” Desborough says. “How do we understand what the positive and negative effects are before we put them into the overall system, so that we aren’t surprised when something bad happens?”

For the U.S. Department of Defense, systems engineering means “planning, analyzing, organizing, and integrating the capabilities of a mix of existing and new systems into an SoS capability greater than the sum of the capabilities of the constituent parts.” Note that according to the Defense Department’s definition, a system doesn’t really manifest itself in its true sense—in terms of producing desired behaviors—without systems engineering.

“Systems engineering has been practiced...
with intent in industries like defense and power generation for decades,” says Rick Schrenker, a systems engineering manager with the Department of Biomedical Engineering at Massachusetts General Hospital in Boston. “The drivers for their earlier adoptions in those domains included rapidly increasing complexity in deployed systems, rapidly increasing rates of change in these complex systems, and costs that spiral out of control in the absence of intentional and formal control. It is so obvious to me that healthcare can learn from these domains. Frankly, anyone in a systems development role in healthcare who doesn’t at least see the need to familiarize themselves with work in other domains needs to get out of healthcare management. Now.”

What could be the practical value of a system, or system of systems, approach in healthcare? Fewer risks to patients, a reduction in costs for healthcare facilities, and greater efficiencies would top the list, according to experts.

Experts suggest 10 systems engineering principles that are relevant to a system, or “system of systems,” environment in healthcare. For all of these principles, there are robust, practical tools, such as matrices, charts, and diagrams, that support systems thinking and management:

1. Use case—a series of comprehensive steps to identify, clarity, and organize system requirements
2. Requirements management—a process of documenting, analyzing, tracing, and agreeing on system requirements and then controlling and communicating system changes to stakeholders
3. Pugh matrix—a quantitative technique, also known as a decision-matrix method, used to establish and rank many criteria, and options for satisfying the criteria, to make system design decisions or choices
4. Quality functional deployment (QFD)—a method to help system designers and planners focus on the needs of users and build these qualities into systems and components
5. Traceability—a method of documenting system and component requirements, including their origins; how requirements are met, tested, and changed; and how changes could affect requirements

6. Architecture (functional and structural) models—methods of modeling how a system functions (its decisions, actions, and activities) and how it is structured. IDEF0 diagrams (an acronym for integration definition), among other architecture modeling tools, can be used to analyze, develop, re-engineer, and integrate systems.
7. Interface design—the application of user-centered design, which focuses on human factors, clinical workflow, user needs, experiences, and interactions with technology. Use cases and sequence diagrams of clinical workflow, for example, are key to informing interface design.
8. Risk management—a process for identifying, prioritizing, and managing risk. In healthcare, ISO 14971 for individual devices and IEC 80001 for connected devices are standardized references for managing risk, but some experts say they are underused by healthcare delivery organizations.
9. Validation—processes for ensuring that devices conform to defined user needs and intended uses, including testing of production units under actual or simulated use conditions. Simulation is a validation tool.
10. Verification—processes for evaluating whether or not the system actually meets the design requirements, specifications, and regulations

“In my mind, systems engineering is as simple as balancing what you’re trying to achieve versus what are the potential unintended consequences of connecting all of these things together,” Desborough says. “How do we understand what the positive and negative effects are before we put them into the overall system, so that we aren’t surprised when something bad happens?”

— Lane Desborough, Medtronic
Achieving Interoperability

Gregory Herr, director of clinical engineering at The Christ Hospital Network in Ohio, drafted this list to describe the changes he’s seen in his job because of the move toward systems in healthcare.

1. Device/system integration with EMR
2. Increased software support vs. hardware support
3. Adoption of change management practices
4. Regulation/oversight requirements
5. Closer alignment with IT services and applications
6. New specialists and roles—changes in the CE organizational structure
7. Intensity and speed of change
8. Greater visibility in organization
9. Capital planning and selection dependent on systems requirements
10. Balancing traditional clinical engineering roles while moving into new systems roles

“Medical professionals can receive data from the system of systems and perform a more extensive trending analysis of a patient or hospital—predicting issues that could arise for a hospital floor during a particular season or when cases have similar data,” says Kathleen Whanger, quality assurance manager with the vascular division at Teleflex Arrow International. Prediction, she explains, is key to reducing risk and cost. More accurate forecasts could help determine, for example, “how many gauzes to order or how many times a catheter will have to be changed.”

And what does this move toward systems thinking mean for HTM professionals in the field? At the very least, it underscores the changing nature of their jobs and highlights the need for new skills and knowledge.

“At the clinical engineer director level, advanced project management skills become necessary,” says Dan DeMaria, director of Bio-Medical Services & Communications with Olathe Medical Center in Olathe, KS. “The ability to manage an interdisciplinary project is critical to success.”

The move toward a systems dynamic also opens the door to HTM professionals playing even greater roles in their facilities.

“Healthcare technology managers will be using the information from practical applications of systems engineering to improve their infrastructures within a particular hospital unit and throughout the entire hospital,” Whanger says. “With this information they can engage in discussions about improving data trending and communication between devices so as to improve overall healthcare to a patient or patients as well as ease the burden on nurses writing information into charts. This will also allow for improved communication between nurses during shift changes as well as better communication between other healthcare professionals at the hospital.”

Raymond Zambuto, president of Clinical Engineering Concepts, LLC, says that what he calls “clinical systems engineers” will need to take on new, specialized roles, in collaboration with other stakeholders, such as IT professionals, clinicians, and manufacturers, in these areas:

• Process engineering
• Data mining and analyses
• Systems modeling and simulation
• Human factors engineering
• Reliability analysis, root cause analysis, and failure modes and effects analysis
• Risk management
• IT service quality management guidelines
• IT and networking technical skills

Systems thinking advocates believe there is an emerging, but largely unfilled, need for systems integrators in hospitals and other healthcare delivery organizations. That role entails bringing big-picture thinking to sociotechnical systems. Moreover, if clinical engineers and other HTM professionals do not step into these new roles, they risk being marginalized by others who can evolve to meet technology needs, Zambuto says.

New skills are required at the technician level as well, DeMaria says. In addition to working closely with or as a part of IT, “we must understand basic networking and have a ‘big picture’ understanding of the entire data flow from medical device to the network to the electronic medical record.”

Plus, he says, biomedical professionals are often in a position of “triaging” reported problems and engaging appropriate subject-matter experts, including network engineers, systems analysts, or communications engineering staff. While HTM staff may not actually resolve problems, they do take ownership of them and ensure resolution.

“It is my expectation that HTM technicians will be more involved in initial trouble analysis of complex interdisciplinary systems,” DeMaria says. “I can envision a day in which HTM will become a tier 2 help desk function. I expect we will be providing
A complicating factor to the systems evolution is the fact that more healthcare is moving outside the hospital setting and involves issues as complex as EHR implementation and alarm management. The systems dynamic will go with that migration.

resources to a unified help desk, which will further blur the lines between HTM, IT, and even communications.”

Some HTM professionals are beginning to use systems engineering principles and tools more deliberately. “I have seen more and more collaboration in working with IT and risk management as we further develop our EMR, medical device integration, and new electronic adverse event reporting systems,” Stiles says. “As we introduced these new systems, we have followed new and unknown implementation and validation processes developed by our informatics groups based on new and different established standards. We are developing workflow strategies now that include our other major support groups—IT, nursing practice councils, pharmacy—during medical equipment management and support activities.

“An acute example,” Stiles adds, “is that we can no longer just take a system down without advance notice to clinicians and IT support. Our actions performed on medical devices now can make a real-time effect on data reaching the EMR interface.”

A complicating factor to the systems evolution is the fact that more healthcare is moving outside the hospital setting and involves issues as complex as EHR implementation and alarm management. The systems dynamic will go with that migration.

What About Risk Management?

Fewer than 60% of healthcare organizations surveyed employ a proactive, technology-related risk management process, according to a 2012 survey of representatives of community hospitals, academic medical centers, and enterprise healthcare systems by HIMSS, with support from AAMI, the American College of Clinical Engineering (ACCE), and the American Society for Healthcare Risk Management (ASHRM) (HIMSS 2012).

Survey respondents indicated that their organizations attend most often to risk management processes for systems that are clearly identified as either biomedical systems or IT systems. “Some questions of ownership of hybrid systems may result in their ‘falling through the cracks’ of risk management,” according to the survey report.

LEARNING FROM OTHER INDUSTRIES

The nuclear power, aviation, petrochemical, and defense industries are farther along in their application of systems engineering principles and tools, experts say. Many acknowledge that healthcare is different from those industries. Patients, clinicians, and healthcare environments have considerable variability, for example, making it difficult to come up with one-size-fits-all approaches.

Still, the experts also believe there are lessons to be studied and adapted from industries that have applied systems thinking for many years, such as:

Standardization—“The aphorism is that if you’ve seen one hospital, you’ve seen one hospital,” Desborough says. “In other industries, Joe doesn’t decide he’s going to land his airplane a little differently than Bob did, or Sally doesn’t say, ‘I’m going to put the fuel rods in my nuclear reactor slightly differently than Billy did.’ Every hospital is its own system, every doctor is his or her own system. I think that’s changing in pockets, and that’s usually the way it is with the diffusion of any new idea.”

Managing requirements, risks, and connections—“The healthcare industry can learn the importance of defining ‘strong and testable’ requirements, defining the architecture of products or family of products, understanding the importance of assessing the risk of a system of systems, understanding the importance of interface requirements between systems, and the importance of testing and tracing those interfaces,” Whanger says.

“Other industries have worked out different ways of making sure that pieces connected together actually work together as intended, while minimizing unintended consequences,” Baird says. “Other industries know how to specify, install, and test connected systems. They also know how to continue working safely when components they are connected to stop working.”

Learning capability and sharing—The ability to learn from a system, and use that learning for continuous improvement, is lacking. Learning capability can be a system behavior—if it is engineered into the system. Likewise, routine sharing of learnings throughout the healthcare community is lacking.

“We can get a sort of ‘peace dividend’ from the set of tools and techniques from other domains,” Desborough says. “We don’t have to go and build a differential algebraic equation solver—we can just go and get one off the shelf that somebody else from another industry has built. The availability of these tools has never been better.”
Who’s Regulating Systems?

Currently, it’s up to manufacturers and healthcare delivery organizations to attend to the potential complications when multiple devices or systems are connected.

“It’s not that regulators are avoiding the issues posed by complex systems,” Schrenker says. “Regulatory professionals were among the parties who advocated for the creation of 80001, and MDDS [Medical Device Data Systems rule by the U.S. Food and Drug Administration (FDA)] is a regulation. Rather, it’s that the laws they are required to enforce were created in a very different technological context. Until consequences emerge that make the risks of the current context evident, regulatory paradigms will not change.”

He believes it will take a serious adverse event that implicates the lack of regulatory oversight for the implementation of a complex system, in which serious risks were not systematically assessed and managed, to change regulations.

“We are assuming support of physician offices, outpatient clinics, and other nonhospital care areas as the hospital builds its healthcare network,” Herr says.

**Systems Applications In Manufacturing**

Systems engineering, architecting, and integration are increasingly relevant to manufacturers in designing and developing health IT equipment.

“There are a number of companies today that have developed or are building competencies in these areas, whereas before there might’ve been functional engineering departments like electrical or mechanical or software engineering,” Desborough says. “It’s a recognition that these things are all part of a broader system and we need to be thinking about these different aspects proactively.”

In Desborough’s own work developing an artificial pancreas, model-based design and simulation are powerful tools. Models and simulations allow designers and developers to accurately predict desired behaviors and unintended consequences of a system—and tweak the system to weed out negative effects—in early stages of design and development.

With such tools, manufacturers can get more “proactively engaged” in designing products to fit into a broader system, Desborough says. Models and simulations are applicable as well to healthcare delivery organizations that are engineering or re-engineering systems. Some healthcare systems, in fact, have created simulation centers for this purpose.

“I also think that many companies are going to have to think defensively about their designs,” Baird says. “Think about when you learned to drive a car. There is a style of teaching that is called ‘defensive driving techniques’ where you anticipate that things will go wrong, and your behavior is to minimize the impact of things going wrong—things like maintaining a safe distance between you and the car in front of you.”

“Similarly,” Baird says, “in other industries that have successfully connected systems together, there are defensive design techniques that minimize the effects of a network that is down, or of a connected component that has failed,” so that no single point of failure takes down a whole system.

Whanger says manufacturers need to broaden their perspective and communicate even more with stakeholders outside their own facilities. “Manufacturers should think about how their device can improve the health of the patient and work with other companies developing other supporting medical devices to develop and define integration points,” Whanger says. Companies also should improve communication between the hospital environments and the company for postmarket surveillance, she says. “They should also realize there could be a market for simpler devices but with the same communication capabilities for hospitals without the technology infrastructure—and also for in-home devices. There are lots of great possibilities by thinking beyond one device.”

In a sign that industry is beginning to recognize these possibilities, the CEOs of nine device makers (Cercacor, Cerner, Dräger, GE Healthcare Systems, Masimo, Smiths Medical, Sonosite, Surgicount, and Zoll) announced in January 2013 that they would work together to make their devices interoperable. Specifically, they will work toward sharing information across different devices to improve patient care—a systems-thinking approach.

**The Impact on Life Cycles**

Managing the life cycle of equipment will require a systems perspective as well. This begins even before purchasing decisions are made. “Obviously there will be more requirements in the request for proposal (RFP) that need to be thought through,” Baird says.

“Healthcare technology managers are going to need to demand more information from...
their vendors, and will need to work closely with the vendors to ensure that everything works together as intended, without unexpected consequences.”

At the purchasing level, there’s a growing list of variables to consider. “The purchasing process needs to take account of the environment, work flows, human factors, and other equipment systems it will be interacting with,” Zambuto says. “The design of medical equipment is a much more complex business if it is to be done right. My concern is that not all manufacturers will recognize these factors, making it all the more important for the hospital and its clinical engineers and BMETs (biomedical equipment technicians), whether in-house or contracted, to be aware of the reality of system of systems interaction.”

In practice, this means that the clinical engineering job of managing medical systems is not only changing, but expanding. “Our clinical engineering program still follows our basic goals of equipment management, preventive maintenance, repairs, and reporting,” Stiles says. “We still report to facilities, as most other hospitals do, but we have created many shared processes with other system owners such as IT, pharmacy, and risk management.”

To work more effectively in this systems environment, Long Beach Memorial Medical Center has adopted different processes to support the acquisition of new equipment, design of medical device integration workflows, and collaboration with new groups and committees, he says:

• A universal workflow and efficiency process based on Toyota LEAN that provides standardized goals and effects for all disciplinary groups and services. This LEAN-based approach has been useful in studying and developing many system-based approaches, such as bar code medication administration, or the introduction of an additional EMR module such as anesthesia workflow. The medical center is now using the LEAN process in all areas of focus. This has helped the institution adopt standardization of system validation, downtime processes, and evaluation of even newer system implementations coming on line in the future.

• The medical system has introduced into its culture the use of its strategic plan in every aspect of employees’ jobs to achieve our goal of matching these systems to work as one.

• A new capital and construction request process now requires review by facilities, IT, and biomedical to ensure that requests meet the new systems approach in infrastructure, technology, and informatics.

Likewise, with a systems approach, medical and health IT upgrades, repair, and maintenance will increase in scope, at least over the short term.

“If there is a software upgrade for one device, this might cause a communication error to other medical devices or cause a communication error to the nurses’ station,” Whanger points out.

The fact that just about everything is connected in multiple ways in the modern hospital is the main point that healthcare

“Medical devices are part of a larger electronic data management system,” Zambuto says. “BMETs need to take account of this in their approach to repair and maintenance protocols.”
— Raymond Zambuto, Clinical Engineering Concepts, LLC

Systems Considerations for Purchasing Decisions

Kathleen Whanger, quality assurance manager with the vascular division at Teleflex Arrow International, provided these system-oriented factors for healthcare facilities to consider when buying medical equipment with communication features.

• How often is the medical device used?

• How does the medical device integrate with the current hospital communication center?

• How does the information from one medical device integrate with information from another medical device?

• How is the information from multiple medical devices relayed to the nurses’ station or to a doctor’s mobile device?

• How is the information from multiple medical devices relayed to the companies building the devices?

• How do the alarms and alerts from the devices impact quality of work for healthcare professionals and quality of stay for patients?

• How transportable are these devices?

• What is the cost to install the equipment, train healthcare professionals, and maintain these interfaces?

• Will the interactions between the devices reduce costs and risks to the patient eventually?

• With software upgrades, does the company understand how the device will interact with other devices?
Technology experts keep coming back to. Virtually no piece of equipment operates in isolation anymore.

“Medical devices are part of a larger electronic data management system,” Zambuto says. “BMETs need to take account of this in their approach to repair and maintenance protocols. For example, the loss of data transfer on a monitoring system could be a hardware problem, a software problem, or a network problem. Coordination needs to be maintained with the IT department. Similarly, when working on a system that supports more than one patient, care must be taken to not disturb the flow of information from other beds while troubleshooting or maintaining a problem area.”

Collaborative efforts like these might not be easy—at least at first. “I like to compare this to cleaning out my garage,” Baird says. “I have so much clutter in my garage right now; when I finally decide to reorganize it, during the actual reorganization itself, the garage looks much worse—everything is moved out of place, piled on top of each other, as things are moved around to make room. Eventually, I get one corner organized, then another, and eventually all of the clutter and chaos in the middle of the garage is gone and I have a much more efficient setup.”

Ironically, it could well be that more systems will help solve some systems issues. At the Christ Hospital Health Network, Herr says the computerized maintenance management systems (CMMS) incorporates more than traditional clinical engineering devices management. It includes IT information and regulations related to the Health Insurance Portability and Accountability Act (HIPAA). “Systems management is part of this CMMS,” he says.

Creating these systems and making them work smoothly won’t happen all at once, and it will be challenging. But there are ways to start. “Let’s just say that without recognizing that we are dealing with a system of systems, and breaking the delivery of care in today’s and tomorrow’s hospitals into smaller ‘chunks’ or subsystems, we will never get a handle on how it all really works or how to improve operations and safety,” Zambuto says. “If we try to treat it as a whole, we will drown in a tsunami of unintended consequences.”

References
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.

**Mary Logan** What forces are driving the integration of medical devices into hospital networks?

**Tom Judd** In patient care, the forces driving it are quality and safety. National studies have shown that nurses spend 35% of their time transcribing device information. It has been shown that getting device information onto IT networks and into electronic medical records (EMRs) automatically can help clinicians reduce adverse events. We need to be able to send diagnostic information from medical devices to IT networks and EMRs. Increasingly, reimbursement of doctors and hospitals is going to be driven by having the right information at the right time.

**Rick Hampton** The push to adopt electronic health records (EHRs) under the American Recovery and Reinvestment Act and the HITECH Act is creating a huge drive for increasing the automation and computerization of healthcare. Alarm management—the need to integrate and rationalize competing alarms from medical devices—is another force driving this integration. In the past, we tried to rely on separate, proprietary networks and it has worked. But there are better productivity gains if we can integrate devices using one system rather than many.

**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.

**Mary Logan** Where is the push toward wireless technologies coming from?

**Ed Cantwell** There is an overarching desire for mobility within the hospital, and eventually out of the hospital. Wireless technologies...
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

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.
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 to look at their safety and efficacy, both of which depend heavily upon network reliability. In response, a lot of the wireless vendors offer solutions based on proprietary technologies, not standards. Those proprietary mechanisms may not interact well with end users, client devices, or any other system.

**Bob Alberte** 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 understand 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 standards¹ are a key building block for risk management in these kinds of systems.

Bob Alberete 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 they turn 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.

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.
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.

Mary Logan What steps can and should healthcare facilities, device manufacturers, and IT vendors be taking to address these challenges?

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.2 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 60601-1-23 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
Hospital network infrastructures can carry critical and sensitive data and therefore become a significant subsystem in a complex interaction of sophisticated systems. In the last decade, healthcare technologies have become increasingly interconnected and codependent. IT networks supporting medical devices that have historically been segregated are now more likely to be combined into one enterprise IT network. This convergence facilitates more capable and connected systems that can drive better care by enabling efficient clinical decision making throughout the hospital, while allowing healthcare delivery organizations (HDOs, such as hospitals) to optimize and leverage a common IT infrastructure. But with all these benefits come new risks that need to be managed. A network’s role in the delivery of care warrants deliberate and purposeful risk management.

In October 2010, the IEC released a new standard titled IEC 80001-1: Application of risk management for IT-networks incorporating medical devices (hereafter called 80001). The goal of 80001 is to manage the risk that comes along with using technology for the benefit of the patient, allowing us to realize the upside of medical IT networks (IT networks in healthcare facilities that incorporate medical devices) while ensuring that any potential risks are controlled and minimized. The standard defines a framework for applying a risk management process to the incorporation of medical devices into shared enterprise IT networks.

**80001 Overview**

80001 defines a medical IT network as any IT network in which at least one of the nodes is a medical device as classified by regulation. It clearly defines positions, functions, activities, policies, procedures, and documentation needed to manage risk during incorporation of medical devices into IT networks. It also requires a comprehensive risk management policy to be put in place to protect three key properties: safety, effectiveness, and data and system security. The standard is addressed to three audiences:

1. The hospital, or HDO, is responsible for owning and managing the overall risk management of its medical IT networks. This entity is referred to as the Responsible Organization (RO) in the standard.
2. The medical device manufacturer (MDM) supports the process by providing information about the medical devices that will allow them to be successfully connected to the network, and also information that will support the hospital’s system-wide risk management of the network.
3. Other providers of IT equipment or services that may not be a medical device also provide technical information to support medical device incorporation and risk management.
Figure 1 shows how these audiences are all involved in risk management of medical IT networks. The standard does not address segregated networks dedicated to one single MDM, either built by or as specified by the manufacturer. These are considered part of the medical device delivered by the manufacturer. Also out of scope is any premarket risk management of medical devices.

Because there are many different organizations and departments—both within and outside the hospital—that are required to engage to support successful risk management, an international standard is considered the best way to organize and maintain this effort.

The requirements set forth in 80001 generally fall into one of these four topics:
1. Roles and responsibilities – who are the different players and what do they do?
2. The risk assessment process itself – an organized way to analyze and evaluate risk
3. How the risk management process fits into the lifecycle of the medical IT network
4. Documentation of all of the above

The risk assessment process itself (Figure 2) is the subject of an IEC technical report scheduled for publication in late 2011 titled 80001-2-1 Application of risk management for IT-networks incorporating medical devices: Step-by-step risk management of medical-IT networks; Practical applications and examples (hereafter called Technical Report 2-1).

Step-by-Step Risk Management
Risk management is a topic rich in theory and has been a source of many intellectual and philosophical debates and discussions. But eventually the time comes to put the right players in a room, put the fingers to the keyboard, apply the procedures, and decide as an organization whether you believe your system is safe enough to be applied to patients. Risk is another language and must be adopted consistently by every member of the risk management team. This language is used to bridge the gap between the native languages spoken by these team members, be it clinical, technological, business, or security. Once the players are assembled and the language is understood, the group must proceed through logical steps to facilitate what is ultimately a hypothetical exercise.

Technical Report 2-1 will provide further explanation of the actual performance of the risk assessment, which is only one section of the 80001 standard. Note that many other requirements specified in 80001 must be met before proceeding with the risk assessment: allocating resources, establishing risk management policies and procedures, defining probability, severity, and acceptability scales (HDO); supplying required network characteristics and relevant hazardous situations (MDM); and supplying network design information, etc, of the network infrastructure components (other providers of IT). Beyond the requirements specified in the standard, the parties may choose to develop responsibility agreements to specify further detail. (For more on responsibility agreements, see the article on page 33).

Fundamental Risk Analysis
The risk management process called out in 80001 is based on a well-established method for risk assessment. Assessment involves three main activities:
- Analyze – identify hazards and estimate risk
- Evaluate – determine acceptability

Risk is another language and must be adopted consistently by every member of the risk management team. This language is used to bridge the gap between the native languages spoken by these team members, be it clinical, technological, business, or security.
Control – implementing designs or procedures that lower risk

As shown in Figure 2, these activities are executed in an iterative fashion until the evaluation determines that the risk level is acceptable.

To fully analyze risk of a system, one needs to clearly define the system under analysis. This involves two aspects:
1. The technical design, details, and scope of the network under analysis
2. The context in which the system is used.

Context includes information such as patient acuity, clinical workflows, existing IT or biomedical procedures, and anything that would aid in the estimation of risk.

Risk is a combination of probability and severity. In other words, something that is likely to happen frequently with minor consequences can be just as undesirable as something that is very unlikely to happen, but has very severe consequences. For purposes of risk assessment, we consider risk somewhat quantifiable, at least in terms of a level of risk. This level is weighed against the benefit of placing the system in to use, and a determination is made as to whether the benefits outweigh the risk. This determination happens in the evaluation step. Typically, risk levels below a certain level are considered acceptable and risk levels above a certain level are considered unacceptable, regardless of the benefit. For the grey area in between, it is more important to weigh the benefits against the risk in order to complete evaluation.

**Terminology**

During the risk assessment meetings and discussions, several people representing different skill sets and interests will speculate on what could go wrong, who or what might be negatively affected if it did, how likely this is to happen, and how severe the consequences could be. These are certainly difficult discussions, but they are nearly impossible if the group does not first have a common language to use. Note that one chain of events in a medical IT network can start with something very technical deep inside the network, and end in something clinical at the bedside or point of care.

The critical terms used in Technical Report 2-1 are hazard, hazardous situation, sequence of events (or cause), and unintended consequence (UC). Figure 3 shows these terms and how they are related to each other. Hazards are categories of things that could be detrimental to one or more of the key properties. Examples are electrical energy, equipment suspended from the ceiling or wall, and, in the case of medical IT networks, loss or degradation of function. A hazardous situation is a circumstance in which a person or the organization is exposed to the hazard. A disconnected Ethernet cable (loss of function) is benign until the time when critical traffic needed to make a time-sensitive care decision is lost due to that failure.

During the risk assessment meetings and discussions, several people representing different skill sets and interests will speculate on what could go wrong, who or what might be negatively affected if it did, how likely this is to happen, and how severe the consequences could be.
cause, also called a foreseeable sequence of events, creates the hazard if it was not already inherent to the system (the disconnection of the Ethernet cable leads to loss of function) or creates the hazardous situation (a broken fixture results in a falling suspended mass). Given the occurrence of a hazardous situation, one can predict possible unintended consequences that may result. Unintended consequence is a more general term for ‘Harm’ which is used in 80001. In the case of safety, this could be physical injury of varying degrees of severity. Note that even when a hazardous situation occurs, it’s not guaranteed that an unintended consequence occurs. For example, an alarm is missed, yet no one is hurt.

The Steps
With the fundamentals of risk assessment established and the terminology agreed upon, we can examine the detailed steps involved in completing the risk assessment of a system, in this case the medical IT network.

Steps 1 and 2 are to identify hazards and causes. Assessing risk involves thinking about all the ways the system under analysis, in this case the medical IT network, can impact the key properties. This thought process can go top-down, in other words, what are the ways this system can be dangerous (hazards), and how could this happen (causes)? Or it can go bottom-up, in other words, what are the things that can break or fail in this system (causes), and how might that expose us to a hazard and become a hazardous situation? There may be multiple causes per hazardous situation and multiple hazardous situations per cause.

Step 3 is to determine possible unintended consequences that may result from each hazardous situation, based on everything the team knows about the system under analysis and the context in which it is used. The team must also assign a severity level to the unintended consequence.

Step 4 is a particularly difficult one. Here the team must estimate the probability of occurrence of the entire chain (error/fault through to unintended consequence).

The estimations in steps 3 and 4 for severity and probability are made using scales that the organization established ahead of time. At this point, the analysis is complete, and risk can be calculated using the values determined in these steps. This calculation follows the organization’s pre-established formula showing risk level as a function of severity and probability (typically a matrix).

In Step 5, the risk level of these hazardous situations is evaluated for risk acceptability, based on the HDO’s pre-defined criteria for acceptability. If it is not acceptable, the HDO can choose to forgo the system or activity that would give rise to this hazardous situation, or the organization can put measures in place to control or lower the risk.

In Step 6, risk control measures are identified. Control measures can be network design decisions, other technical methods, or they can be procedural, warnings, etc. They may lower risk in one of several ways: by lowering the probability that the event happens, by lowering the probability that an unintended consequence occurs given the occurrence of the hazardous situation, or by lowering the severity of the unintended consequence.

Steps 7 and 8 are to implement and verify the risk control measures. Implementation involves building the network infrastructure to include the design mitigations identified, label it accordingly, and instantiate procedural mitigations, etc. Then it must be verified (checked) that the mitigations are in fact included in the final system. Verification also includes checking the effectiveness of the mitigation. Execution of this step will vary depending on the type of mitigation. Design mitigations can likely be verified to be effective in a test lab. Procedural or workflow mitigations can be evaluated theoretically, and then monitored in the live phase of the network.

Step 9 is to determine if any new risks arose during the process of mitigating the original list of risks. For example, very strict security measures may have been proposed, but these may lead to a situation in which a clinician cannot access data or functionality from a critical system in an emergency.

And finally, in Step 10 the overall residual risk is evaluated. Once everything is complete, each hazardous situation identified may have a residual risk associated with it. These should be evaluated in aggregate for overall acceptability.

Relationship of Multiple Risk Analyses
Medical IT networks are complex, highly dynamic super systems of medical devices and IT equipment. While risk must be shared and ultimately controlled by those who own and maintain the network, it is important to ensure that there is appropriate information flow between the hospital, medical device manufacturer, and other IT providers such that a thorough risk analysis can be completed.

Applying risk management at a subsystem level is no small task. Converging multiple subsystem risk analyses is difficult, and the complexity increases significantly at a super-system level, particularly when the systems are delivered by multiple companies and organizations, as is the case with medical IT networks.
Timing of Risk Analyses

While it may be understood that each of the three target audiences for the standard have a part to play in the overall risk management of the final system of systems, it is important to understand how these risk analyses relate to each other, particularly for the MDM and HDO who both execute independent risk analyses. The notion that HDO risk analysis in relation to MDM risk analysis “picks up where the other left off” is a bit of a misnomer. Rather, they are analyzing the same hazards with respect to the medical IT network.

Both the MDM and the RO perform risk analyses, as shown in Figure 4. Each are analyzing the risks associated with incorporating the medical device into an IT network, or the “IN USE” portion of the timeline shown here. MDM activities are shown above the timeline, HDO activities are shown below. The actual topic of both of these risk analyses is the “IN USE” portion.

Medical device manufacturers recursively perform risk analysis during product development, from conception through design and testing. Typically, this is per ISO 14971. This risk analysis encompasses everything that could be hazardous about the device in its intended use or foreseeable misuse. One portion of this includes risks associated with operation of the device on a network.

At the point where the risk analysis shows the overall risk to be at an acceptable level per the MDM’s risk policies, the design may proceed to market (after any required regulatory clearance).

Responsible organizations recursively perform their risk analysis during the project intended to incorporate the device into the enterprise network. During this process, information from the MDM is used. First, a list of required characteristics of the network (i.e., what does it need to be/do to support the device connection) is used to ensure that the network can support the device. Secondly, a list of MDM-identified potentially hazardous situations specifically related to incorporation of this device into the network can be used as one source of input during Steps 1 and 2 (Identification of Hazards and Causes). All of this information is provided so that the HDO can properly estimate and manage risk. For example, the MDM explains how the device will react in the case of a lost connection. It might alarm or somehow notify the user of this condition. The HDO may determine that this situation is detectable and no further risk control is required, or they may choose to add further risk control measures to the network to reduce the possibility of a lost connection. The HDO will also use information from the network equipment or service providers to support the risk assessment, such as mean time between failures data, test strategies, failure modes, best practices, etc.

At the point where the risk analysis shows the overall risk to be at an acceptable level per the HDO’s risk policies, the medical IT network may go live.

Content of Risk Analyses

Now consider the actual content and topic of both risk analyses. Both the MDM and the HDO are analyzing the risk of hazardous situations related to the fact that the medical device is functioning on a network once it is live and in use, presumably using the network connectivity for some functionality. Both the MDM and the HDO are identifying hazards and hazardous situations, speculating on possible causes and potential resultant harms or unintended consequences that exist once
### Table 1. Simplified summary explanation of timing and content of medical IT network Risk Analyses

<table>
<thead>
<tr>
<th>Question</th>
<th>Medical Device Manufacturer</th>
<th>Responsible Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>When is risk assessment performed?</td>
<td>During product development (pre-market)</td>
<td>During medical IT network project execution (pre-go-live)</td>
</tr>
<tr>
<td>What is the subject of risk assessment (relevant to 80001)?</td>
<td>Networked operation of the medical device</td>
<td></td>
</tr>
<tr>
<td>Where can potential mitigations be applied (design, protective measures, labeling)?</td>
<td>Medical device</td>
<td>Network infrastructure</td>
</tr>
<tr>
<td>What is treated as a black box during risk assessment with general failure modes?</td>
<td>Network infrastructure</td>
<td>Medical device</td>
</tr>
</tbody>
</table>

Common system-level failure modes that should be considered by the MDM. Causes of these failure modes are considered and mitigated by the HDO.

- **Intermittent connectivity:** intermittent dropped packets without complete connection loss
- **Lost connectivity:** connection completely lost for a sustained period
- **Loss of control:** attacker utilizing network security vulnerability to take control of the system or render the system unusable
- **Corrupted data:** bits flipped or dropped during transport
- **Incorrect or inappropriate timing of data:** The network delay or jitter (i.e., variation of delay) exceeds expected or allowable limits
- **Foreign packets:** unrecognized packet type or failure parsing
- **Excessive packets received:** from broadcast or multicast storm, UDP flooding, denial of service, or any other reason
- **Exposure of Private Data:** how might private data be compromised?

The medical IT network is in operation. There are three main differences between these two assessment activities:

1. The policies and procedures governing the risk analyses. As there is no single universally accepted way to specify probability, severity, or risk acceptability, these are specific to the organization.
2. What is known about the context of the medical IT network. An MDM may provide a device in many different markets or segments with varying use cases, workflows, and network designs, whereas the HDO can more clearly specify the context of the use of the medical IT network, including specific workflows, procedures, typical user and patient profile, and network availability.
3. Where in the overall system each organization has the power to apply risk control measures, as discussed below. The MDM may apply design and labeling mitigations to the medical device. The HDO may apply design and labeling mitigations to the network itself, or to the procedures and workflows associated with it.

**Scope of Risk and Control**

As mentioned above, one of the main differences between these two risk assessments is the degree of control over each of the subsystems that make up the entire system under analysis.

As an MDM develops products intended to operate on shared, general-purpose networks such as hospital enterprise IT infrastructures, cellular networks, Internet, etc., the network will have to be treated as a black box having certain system-level failure modes (see sidebar). These should be considered as causes or foreseeable sequences of events. Typically they will lead to hazardous situations within the category of lost or degraded function.

As an HDO develops an enterprise network, the devices to be incorporated will have to be treated as black boxes with certain network requirements and behaviors, including behavior in the presence of a network failure. The HDO will consider the same system-level failure modes (see sidebar). However, with ownership of and insight into the network infrastructure design and operation, these failure modes must be further broken down into more specific causes. For example, lost connectivity may result from an overloaded link, network hardware failure, network software (OS) failure, improper QoS configurations, overly aggressive security, faulty cabling, accidental disconnection of cabling, power loss, EMI, etc. Each of these more specific causes can be evaluated for probability of occurrence, and each may have specific risk control measures applied. This is an important step in the risk management process because reducing the probability of the failure is a very effective way to reduce risk.

In terms of risk control measures, the HDO is not in a position to apply mitigations to the networked device other than by controlling configurations and workflows. Rather, the HDO can implement mitigations in the design or labeling of the network infrastructure.

Conversely, the MDM is not in a position to apply mitigations within the network to reduce the probability of these failure modes. Rather, the MDM can implement mitigations in the design or labeling of the device.

**Layers Within a System of Systems—Locations of Errors and Faults**

Part of risk analysis involves considering all the ways the system (in this case the medical IT network) can fail. To do so, an understanding of the layers that make up the entire system is important, as well as what types of errors and faults could exist at each layer. The medical IT network can be considered in two general layers, the network infrastructure...
(switches, routers, APs, cables, etc.), and the devices connected to it (servers, hosts, medical devices, etc.). In each layer there are subsystems (individual components) and systems (subsystems working together). The network infrastructure system would be all of the network components (switches, routers, APs, etc.) working together to transport data between the connected devices.

Each layer can then be taken independently and examined for errors and faults. Errors in either layer may be functional (the system does not do what it is expected to do) or performance related (it fails under loaded or edge conditions). Additionally, the overall system and the interactions between the layers (interoperability) must be considered.

As the HDO is assessing risk in the network infrastructure layer, there are two categories of faults to examine.

1. Faults that are outside of HDO control.
   These are either errors that existed in the devices upon delivery to the HDO (e.g., software error in the operating system of a network component) or failures that occur during usage (port hardware failure or power supply failure). Information from the IT device manufacturer as well as pre-go-live testing can expose these possible faults and help identify workarounds.

2. Faults that are within control of the HDO or network designer/owner/maintainer.
   These include network design, topology, and configuration. An overloaded uplink or improper AP spacing are examples. It is the responsibility of the HDO to verify that the network design is correct and appropriate given the information from the network infrastructure component supplier and the MDM.

Enabling these complex interactions between networked hospital systems requires sophisticated risk management. All parties involved must understand the interactions between the systems, how the risk management efforts relate to each other, and how to collaboratively design the system and manage the system risk.

Reference
AAMI Guidance
For Healthcare Providers
Managing Medical IT-Networks


Order Code: 8000101 or 8000101-PDF
List $120 / AAMI member $60

TIR80001-2-1:2012, Part 2-1: Step by step risk management of medical IT-networks; Practical applications and examples
Order Code: 800010201 or 800010201-PDF
List $130 / AAMI member $65

TIR80001-2-2:2012, Part 2-2: Guidance for the communication of medical device security needs, risks and controls
Order Code: 800010202 or 800010202-PDF
List $130 / AAMI member $65

Order Code: 800010203 or 800010203-PDF
List $120 / AAMI member $60

TIR80001-2-4:2012, Part 2-4: General implementation guidance for healthcare delivery organizations
Order Code: 800010204 or 800010204-PDF
List $100 / AAMI member $50

Order your Copy Today!
Call +1-877-249-8226
Visit http://my.aami.org/store
Safety Innovations

Best Practice Recommendations For Infusion Pump-Information Network Integration

Pump integration requires pervasive and reliable wireless coverage—if pumps can’t communicate with the server via a wireless network, no integration can occur.

**Introduction**

Closed-loop medication administration with infusion devices is being driven by the healthcare community in order to improve patient safety and to meet electronic health record (EHR) goals under the Meaningful Use provisions of the ARRA-HITECH act. Therefore, hospitals are exploring the following infusion pump functionalities that not only can reduce errors thus improving safety, but also reduce manual data entry:

- **Auto-programming**, in which orders are sent to the pump to be confirmed by a nurse before starting infusions
- **Auto-verification**, in which a nurse manually programs the infusion pump and then the programming is checked against a medication order
- **Auto-documentation**, in which pump programming, status, and alerts are automatically fed into the patient’s electronic medication record for confirmation
- **EHR alerting systems** that bring together diverse patient information and pump data to generate combinational alerts in near real time

Although these integrative processes and functionalities facilitate accurate, timely, and complete charting of medication infusions, only a handful of healthcare facilities in the United States have adopted one or more of them. Why is integration of pumps with electronic/information systems so slow to take off? In this paper, authors provide current barriers to closed-loop medication administration and offer best practices from some of the early adopters.

**The Must-Haves and Must-Dos for Pump Integration:**

Infusion pump integration rests on five specific infrastructure requirements, which must be in place before a facility can move forward with any integration plans:

1. Reliable, pervasive, and secure wireless connectivity;
2. Electronic medication orders containing all infusion parameters;
3. High compliance with bedside barcode scanning for medication administration;
4. Electronic repositories for administration data; and
5. A highly reliable method of associating a pump channel with a patient and a medication.

Today’s infusion pumps typically use wireless communication with a pump server or gateway. Wireless networks need to be pervasive, highly reliable, and offer adequate security protection and many facilities are often not ready to provide this level of wireless security protection.

One of the strategic decisions hospitals have to make when integrating infusion pumps to the network is whether or not the available technology meets the organization’s requirements for information security.
coverage. Some facilities (e.g., Veterans’ Administration) need to comply with FIPS requirements for wireless security, which require support from the facility, pump supplier, and router/server suppliers. One approach to addressing security concerns is for patient specific information to be documented and contained “outside” the pump (i.e., at the pump server or EHR level). If the pump does not contain a patient ID, medication order number, or other patient identifying data but only receives programming information, sends delivery information, serial number, and channel, the data transmission between the pump and its server may not comply with FIPS requirements.

Pump integration requires pervasive, reliable, and secure wireless coverage—if pumps can’t communicate with the server via a wireless network, no integration can occur. However, facilities vary widely in wireless coverage and signal strength, and facilities need to make sure their systems can still function during times when the pump is out of communication or the pump server is unavailable. Infusion pumps typically have cache-and-forward capabilities to prevent data loss, with sufficient memory to store pump information until the pump can re-connect. Additionally, most wireless pumps have notification capabilities when communications between the pump and the server are lost. These notifications can be in the form of a visible icon on the pump showing that data transmission was interrupted or as a message directly from the server indicating interruption.

Although a “gold standard” approach to wireless integration would include assessment of coverage and potential interference at all bed locations, this may not be feasible for all facilities. One rough method of quickly assessing wireless coverage is through the support and use of voice over internet protocol (VOIP) communication devices. If patient care areas in the facility have been shown to offer adequate coverage and uptime for VOIP use, it is likely that they will offer sufficient support for infusion pump integration. Even after a wireless environment is made ready for networked pumps, facilities need to monitor their networks for “jamming” or other malicious activity that could prevent pervasive and timely wireless transmission, and also routinely assess the impact that pump “traffic” itself is having on the network.

Along with adequate wireless coverage, facilities need prompt and seamless support from EHR and pump suppliers, especially when it comes to troubleshooting and site-specific customization during and after implementation. While pump suppliers generally view medical device integration (MDI) as a business driver (and therefore worthy of the time and effort necessary for a successful implementation), the story can be quite different when it comes to EHR suppliers. Be aware that many suppliers prioritize MDI far behind other initiatives like ancillary site support or public health reporting.

Food for Thought

The long life of infusion pumps, 7 to 10 years, reduces the window for the adoption of pump integration. Generally, the ability to implement integration is only available in the latest pumps. The opportunity to accomplish integration, therefore, must be planned as part of the budgeting process for new pumps and EHR software.

It would be wise to buy integration-capable pumps even if you are not ready to integrate. If you don’t, you could wait a long time before you can integrate your pumps with your data or information network(s).
To support the integration champion, establish a standing department that is responsible for Medical Device Integration (MDI) and is led by the integration champion. An integration team should be established that consists of representatives such as nurses, physicians, pharmacists, clinical program managers, dieticians, medical informatics professionals, medical researchers, risk managers, HIM, quality improvement managers, IT managers, purchasers, and clinical engineers. The size and makeup of the team should be adjusted according to the integration project. Such a group should have the following duties:

1. Identifying devices that have information that is useful to clinicians
2. Setting clinical priorities for integration
3. Overseeing design and development, making sure that the integration of pump devices into documentation and alerting systems meets the requirements of all care areas using pumps
4. Budgeting for development and equipment purchases
5. Purchasing specifications and assistance for new devices
6. Installing new or updated software to support device integration
7. Ensuring ongoing maintenance for installed device integration systems and collecting and analyzing data on the efficiency of installed systems.

After BPOC/CPOE, a champion with a mandate, and a team of support have been achieved, then proceed with readying your devices and systems.

RECOMMENDATIONS

Regardless of whether a facility is selecting new suppliers or attempting integration with existing suppliers, the following steps should be taken.

1. Device readiness
   - Purchasing authorities in your facility must buy the appropriate devices and interface equipment.
   - Clinical Engineering and IT must be able to support the connected devices.
   - Equipment management must be able to supply enough equipment to areas that use integration. It is confusing to have only some of the equipment (of the same type) capable of interface.
   - Devices should be identified and labeled with a short 4 or 5 digit asset number (not the serial number) that is human readable (and rememberable) and scanable to facilitate ease of use during integration. The asset number should ideally be programmed into the device and is separate from the serial number. Clinical Engineering and Equipment Management are responsible for maintaining the labels.

2. Pharmacy readiness
   - Move towards radical standardization on concentrations and formulations towards a goal of one or two concentrations that support “most” (98%) patients.
   - Ensure that CPOE, pharmacy, pump drug libraries, and other related systems reflect this new formulary and establish a plan for updating all systems in response to formulary changes.

3. IT Infrastructure readiness
   - Assess and upgrade wireless coverage in care areas and pump storage locations.
   - Assess and upgrade database infrastructure.
   - Assess server/client hardware and software requirements.
• Create an information security and privacy policy that you can send to suppliers whose devices or systems include protected health information.
• Determine wireless capabilities and identify potential interference sources.

4. Nursing readiness
• Study and describe current infusion administration workflows in various care areas. Keep these observations in a document that you share with pump and EHR suppliers.
• Develop use cases for pump integration that cover infusion pump use in all areas. Keep these observations in a document that you share with pump and EHR suppliers.
• Establish a plan for compliance monitoring over time.

5. EHR readiness
• BPOC system needs to be able to accept a scanned-in pumping channel during the “5 rights” bar code scanning process. This is the most efficient way for the EHR to link the patient, the IV medication and the pump, and will probably require an upgrade or update to the BPOC configuration and workflow.
• Pharmacy-verified electronic orders must be available to the BPOC system that includes pump programming parameters.
• The system has to be able to receive pump data from the pump server and integrate it into infusion charting and the patient record.

Conclusion
Although infusion pump and network integration has been slow in the U.S., it will likely remain a high priority for healthcare facilities to improve patient care and to comply with the Meaningful Use requirements. It was the intent of this white paper to outline the major steps to successful integration and to emphasize the need for pervasive and highly reliable secure wireless networks that offer adequate security protection, electronic medication orders containing all infusion parameters; high compliance with bedside barcode scanning for medication administration; electronic repositories for administration data; and a highly reliable method of associating a pump channel with a patient and a medication.

RECOMMENDATIONS

Document Baseline Alarm Conditions.
At Johns Hopkins, the conditions were:
• 58,764 alarm conditions, or 350 alarm conditions per bed, per day in 12 days
• 20,158 auditory alarm signals in 8 days for 17 beds in the PICU
• 157 apnea alarms, 90% were thought to be false
• 771 alarm conditions per bed, per day on average in one ICU

Recognize the Contributing Conditions.
At Johns Hopkins, the conditions were:
• Alarm parameters were not set to actionable levels
• Alarm thresholds were set too tight resulting in too many false positives
• Staff working in large clinical units did not have clear accountability to respond to alarm conditions
• Patient rooms with closed doors made it difficult for staff to hear alarm signals
• Too many duplicate alarm conditions desensitized staff to alarm signals
• Lengthy time-lags between installation of devices and staff training on those devices did not allow for staff to become accustomed to the auditory alarm signals of new equipment.
Health Information Technology Collection: A Biomed’s Guide

This comprehensive CD includes more than 200 articles from AAMI publications, specifically on major IT issues in the medical profession.

It examines:
- Device connectivity
- IT Security, bots, malware, and spyware
- Integrating patient data
- Network management and applying 80001
- Picture archiving and communications systems (PACS)
- Radio frequency identification technology (RFID)
- Networked medical devices
- Bluetooth wireless technology

The CD features a detailed glossary of terms, and a convenient search function.

Order Code: ITCD
List / AAMI member: $160 / $85

Order your Copy Today! Call +1-877-249-8226 or visit http://my.aami.org/store
Move Your Healthcare Technology Career Forward

Education
News
Medical Device Standards

Career Growth
Networking
Leadership

Join AAMI and receive:
• Subscriptions to AAMI publications;
• Opportunities to serve on AAMI committees;
• Access to listserves and members-only content on aami.org;
• Discounts on AAMI products and educational offerings;
• Free posting of your resume and 50% discount on online job postings;
• Networking events;
• and much more.

Attention Students and New Professionals!
Receive discounted membership dues!
Reference the Individual Membership Application for more information.

Joining is Easy!
Become a Member
www.aami.org/membership