Even as medical devices and information management systems converge, the information technology (IT) networks into which they’re being integrated are both complex and constantly changing. The recently approved international standard ANSI/AAMI/IEC 80001, Application of risk management for IT networks incorporating medical devices—Part 1: Roles, responsibilities and activities aims to ensure both the delivery of safe, high-quality healthcare, and the security and privacy of patient data in this rapidly changing environment.

The new standard, often simply called 80001, recognizes that cooperation is required between healthcare provider organizations, medical device manufacturers, and IT vendors; identifies the necessary roles and responsibilities; and outlines a process for managing the risk posed by the incorporation of medical devices into the IT infrastructure of the healthcare delivery organization.

Now that the standard has been published, what comes next? AAMI recently spoke with a group of experts who talked about why the standard was developed and offered insight and advice on its implementation.

Sherman Eagles: December 2005 is usually used as the starting point of the work on IEC 80001, when Brian Fitzgerald called a meeting at the U.S. Food and Drug Administration (FDA) to talk about issues with medical devices on IT networks. What factors led up to that meeting?

Brian Fitzgerald: The early beginning of the standard goes back to 2001, when some device manufacturers in Germany started asking about doing something to address problems with their devices not working on hospital networks. After sometimes extensive investigation, they were finding that the problem actually was with the network or with interactions with other devices on the network.

At a 2001 standards meeting in Germany, a group of medical device manufacturers and regulators, including me, were invited to go to a hospital in order to see how this particular hospital system had been adversely affect-
ed in its operations by having segregated networks. Their call to the medical device manufacturing community was to stop the vertical integration of the products and try to integrate all medical devices horizontally into existing IT networks. They were struggling with having to maintain these separate networks. That tour caused everyone to think about what it would take to use traditional IT networking rather than segregated networks for devices.

Then, in 2003, a series of well-publicized cyber attacks on West Coast hospitals caused FDA to begin developing a guidance document on security for medical devices. That guidance document was addressed only to medical device manufacturers, but was of keen interest to healthcare providers and network operators. As part of the rollout of that document, I began to go out on the road and attend some provider conferences. It became very clear to me in 2004 that there was a tremendous cultural gulf between the IT community and the biomedical community. Nothing was then available to address the gaps that existed inside the healthcare provider organizations. And so, in a December 2005 meeting, I pulled together a diverse group of people to begin considering development of a standard. We found that there was a need for the standard, and the German National Committee also thought that it was time for a new guidance proposal. That’s how 80001 was born.

**Steve Grimes:** From the provider’s perspective, we began to notice an increasing number of incidents related to these network systems in the 2003–2005 timeframe. A

---

**Roundtable Participants**

- **John Collins** is director of engineering and compliance with the American Society for Healthcare Engineering (ASHE). E-mail: jcollins@aha.org
- **Karen Delvecchio** is a lead systems engineer for patient monitoring networks for GE Healthcare developing network infrastructure and networked-client capabilities with emphasis on risk management. E-mail: Karen.Delvecchio@med.ge.com
- **Martin Ellis** is patient safety director with BT Health. He has been leading the implementation of BT’s clinical safety management system for the development and implementation of eHealth systems in the UK and internationally. E-mail: martin.ellis@bt.com
- **Brian Fitzgerald** is a deputy division director with the U.S. Food and Drug Administration’s Center for Devices and Radiological Health. E-mail: brian.fitzgerald@fda.hhs.gov
- **Steve Grimes** is chief technology officer of Linc Health and a member of the IEC joint working group that developed IEC 80001. E-mail: Stephen.Grimes@LincHealth.com
- **Nick Mankovich** is senior director of product security and privacy with Philips Healthcare. E-mail: Nick.Mankovich@Philips.com
- **Doug Martin** has been project manager at Carilion Roanoke Memorial Hospital for over 13 years and leads projects that span across information technologies. E-mail: dpmartin@carilionclinic.org
- **Chris Riha** is director of clinical systems engineering at Carilion Roanoke Memorial Hospital. E-mail: cdriha@carilionclinic.org
- **Charles Sidebottom** is director of corporate standards with Medtronic, Inc. and served as secretary of IEC Subcommittee 62A, one of the parent committees of the joint ISO and IEC working group for IEC 80001. E-mail: charles.sidebottom@medtronic.com
key contributor to the problem was the bifurcated nature of technology support within hospitals. Typically, IT took care of networks and clinical engineering took care of medical devices. As an increasing number of medical devices appeared on IT networks, we began to see problems associated with these “systems of systems.” Without a collaborative framework for IT and clinical engineering to work within, there weren’t appropriate means of support or even means of identifying the source of the real problems.

There were existing standards covering the support of medical devices, but these didn’t address issues that would occur once you put those medical devices on a network. We needed to find a way to put effective support mechanisms in place to identify and mitigate against these increasingly complex “systems of systems” problems. Providers were recognizing that these new problems weren’t just isolated incidents; they were part of a growing systematic problem.

Karen Delvecchio: A key trend was the movement of medical devices from proprietary, segregated networks to converged, larger, and more complex networks. The industry as a whole moved in that direction in order to use technology to do what’s best for the patient: getting the data to the right place at the right time. One of the goals of 80001 is to balance the risk that comes along with doing the right things for the patient, to allow us to realize the upsides of this integration while ensuring that any possible risks are controlled and minimized.

Todd Cooper: How does 80001 address the needs of healthcare providers and device manufacturers, which have only increased since development of 80001 began?

Eagles: Over the course of its development, the standard has changed significantly. It has transformed from a medical device standard into a network standard. As we progressed through this development, it got more and more focused on what was happening in the hospitals and on the networks, addressing the problems that were seen there.

Chris Riha: This standard has gained more importance because of the increased need to integrate information from different medical devices into the clinical information system. That has forced us to break down the silos between IT and clinical engineering, and increased the need for IT security.

Delvecchio: I see this standard addressing the needs of all its audiences by providing a neutral construct within which a lot of different groups can collaborate. Developed by both industry and provider representatives, it is neutral by definition. It doesn’t come from one side or the other: IT department or CE department within the hospital, or providers or device manufacturers or IT companies. It came from all the stakeholders that have to take a part in risk management.

Risk management by definition is subjective and in-

About IEC 80001
ANSI/AAMI/IEC 80001, Application of risk management for IT networks incorporating medical devices—Part 1: Roles, responsibilities and activities was adopted as an American National Standard in October 2010. The standard, in development for nearly four years, has far-reaching implications for risk management in the industry. It offers a process for how healthcare organizations can manage risk and consider potential impacts on patient safety in an environment where more medical devices are being attached to information technology (IT) networks.

Medical device manufacturers and IT vendors have a role in this standard by supporting the risk management activities of the healthcare provider organizations.

A myriad of resources are being developed to help hospitals and biomedical departments implement 80001-1, including:

- A manual being developed by AAMI on how to comply with the standard. The manual is scheduled to be published in February 2011.
- Courses and webinars from AAMI to provide guidance
- Technical information reports from the joint IEC and International Organization for Standardization (ISO) working group that developed the standard

To order IEC 80001-1, call (877) 249-8226 or visit the AAMI Marketplace at http://marketplace.aami.org. List price $100, AAMI member price $50. Order code 8000101 or 8000101-PDF, source code PB.
Involves some speculation. This standard establishes a language and a prescriptive set of tasks for the entire process. Instead of everything being vague, it’s more constructive and definitive.

Cooper: How would you advise healthcare providers to start implementing this standard?

Grimes: One of the first things people need to do is inventory their systems. What is the scope of the challenge they’re dealing with?

Another early effort will be engaging critical stakeholders. Obviously, one of the first major stakeholders you’ve got to engage is the leadership. You’ve got to convince the leadership of your organization that this process merits the kind of resources that are going to be required to implement it. You also need to engage the other critical stakeholders, including IT, clinical engineering, and users. Others will also be involved, including risk management, quality control, purchasing, and manufacturers. Begin thinking about how to go about engaging all of those stakeholders.

I think we all recognize that this standard represents a best practice. But, to ensure its implementation, we also need to get buy-in from other organizations like the FDA and The Joint Commission. The weight of these organizations behind adoption of this standard will facilitate our ability to get buy-in within our own organizations. It will help providers get buy-in from their leadership, and get them to agree to provide the kind of resources and attention the standard deserves.

Nick Mankovich: I’m advising providers to gather a core group of interested parties, including an IT person, a biomed person, and a clinical person. This very small multidisciplinary team should get together, read the standard, and try to write a medical IT network

One of the goals of 80001 is to balance the risk that comes along with doing the right things for the patient.
—Karen Delvecchio

“Connecting Quality People, Quality Service”

Biomedical Instrumentation & Technology
agement policy for their organization. They should internalize it, rather than immediately start thinking about what systems to do this on. Once they have internalized it, they will understand how it maps into their own way of working. They can then start talking to vendors and about what their roles should be, so they will get some idea about shared responsibility.

After they’ve gone down that road along with a bit of socializing it internally and with vendors, then they can consider where to start. Can they find a very simple system that a hospital can start doing this risk management on, like a new network installation or a simple network where they’re adding a single device?

I’m finding that providers agree that there is some practicality in bringing an international standard in-house and then rewriting it so it makes sense under house rules.

_Delvecchio:_ I agree that it’s important to engage all of the stakeholders. As we’ve seen, we’re talking about systems of systems. A chain of adverse events can start in the medical IT network with something that could be very technical and deep inside the network, but in the end it affects something clinically at the point of care. That’s why these issues cross different departments and functions within the hospital.

It is understandable that there might be some confusion about this standard. The medical device manufacturer must consider that chain of events and how it might mitigate those risks inside the medical device before it ever gets to market. That same chain of events also needs to be considered by the network owner or maintainer. That’s why they need information from the medical device manufacturer on how the device behaves in these kinds of situations. We’re both considering a particular chain of events—meaning some kind of network failure—but where we’re placing the mitigations is different.

Starting small and choosing a new project or a new portion of the network is a great idea. You could also start with a small list of hazards like the top three things that you want to consider in a network, maybe lost connectivity, incorrect data, or some security provision like unauthorized access. Or you could start with a small list of faults, from the bottom up. What are the top three or four things that could go wrong? Maybe network hardware failures, misconfiguration, or timing of network maintenance. Or starting from the top, is the network design capable of managing the load of devices that we’re expecting it to manage?

_Riha:_ We’ve already gotten started using the standard to redesign our IT security planning process for medical devices. This effort became a necessity when we were hit with a virus about a year ago. Fortunately the virus didn’t really affect our medical devices—which was dumb luck—but it certainly was an eye-opening experience. It forced us to really look at our security processes and policies at an enterprise level, not just with medical devices. We realized that the medical devices were out there, and we had a liability in that. The standard gave us a very helpful tool to focus our effort to improve our policies and procedures.

_Cooper:_ What impact is this standard going to have on medical device manufacturers?

_Charles Sidebottom:_ First of all, there’s the technical impact on the medical device manufacturers in terms of the information that they need to provide to healthcare facilities. We’ve worked very hard to minimize that

Figure 1. Security Characteristics in Draft Technical Report
impact. In other words, the requirements in 80001 that are specific to the medical device manufacturer are, for example, the same as the requirements in IEC 60601-1, Medical electrical equipment, Part 1: General requirements for safety and essential performance. We have tried to keep those requirements in line so that the 80001 doesn’t become a certification standard for manufacturers. Early on, many medical device manufacturers were concerned that 80001 would be just one more standard that they would have to certify to.

In addition, it’s important for the manufacturers to have a way to interact with their customers on these issues. I’m telling people inside our company that they need to understand the standard and what it requires for the implementation of the system so they can talk to their customers about these issues.

**Delvecchio:** Much of the information required by 80001 is available; we just need to collect and distribute it, and make sure that we can present it in language that supports 80001.

Two sets of information are required from device manufacturers. The first are the technical required characteristics for the network, because the standard acknowledges that planning, design, and premeditated incorporation of devices into a network is one of the most effective risk control measures.

The second set of information we’re collecting for all of our network-attached devices is the device behavior: how the device would behave in the presence of a network failure, or if the network does not meet the specified characteristics.

Beyond collecting information, our other challenge involves investing time and resources into educating our customers and ourselves about the standard and compliance, and how each end is responsible for this collaborative risk management.

**Mankovich:** Manufacturers are required to provide information on three key properties: safety, effectiveness, and data and systems security.

From our perspective, we’re trying to keep the 80001 compliance process aligned with ongoing 60601 processes. From the point of view of safety and effectiveness, the challenge in preparing for 80001 is to take information which is already present in almost all of our documentation and aggregate it in a meaningful way that will serve the user in their risk management of a medical IT network. The first chore is really aggregating existing information across all of our manuals, service manuals, and other documentation. We will have to undertake some pilot projects with customers in order to find the best way to do that. We’re not quite sure how the healthcare organizations are going to use this data or to what extent they’ll need deep detail.

Providing adequately detailed information on data and systems security is a little more problematic. The 19 security characteristics that are detailed in the technical report (as seen in Figure 1) is more detail than most of us have been giving customers. We have the information, but most customers have never asked for that kind of detail.

The broad security characteristics are detailed in the IEC Technical Report for Security that is now being circulated among standards organizations. They include areas like audit controls, automatic logoff, emergency access, etc.

We may give this information as part of a request for proposal (RFP) or as our answer to a customer-created security questionnaire, but, in general, it’s quite a bit more detailed than what we have offered in the past. We are working out exactly how to properly address those 19 security characteristics with a more detailed list that will be useful in a risk analysis. We want to be sure that the user clearly understands what risks might have to be mitigated locally by the healthcare organization in their IT integration project. Our newly created security content goes beyond just aggregating from existing customer documents. We recognize the need to provide some new insight and more detailed information to users in a package that’s called the 80001 package. We’re currently moving in that direction, undertaking pilot projects and aggregating information to serve what we think is going to be customers’ needs for risk management information.

**Cooper:** Now that the 80001 standard is published, what challenges do we face in getting the word out about it?

**Sidebottom:** Until very recently, many in the clinical engineering and the IT community knew very little about 80001. Now that it’s published, an education effort is
required to spread the word about it and prevent misinterpretations.

**John Collins:** I think there’s going to be a major problem with education of provider facilities with regard to this standard. I serve as the frequency coordinator for the Wireless Medical Telemetry Service (WMTS). We’ve been trying to educate people about WMTS since 2002 and we still find hospitals that either do not know about it or do not really care if they’re registered or not.

I find the major problem outside of larger hospitals is the combination of ignorance and apathy on the part of the clinical engineering and biomed programs across the United States. While I have about 2,500 hospitals registered with Wireless Medical Telemetry, there are at least 1,000 or more installations given to me by manufacturers that are not registered.

I’ve tried a number of different tacks. I have contacted the biomed departments directly and gotten maybe 5% response. I’ve also contacted the risk management and materials management people at hospitals. And, again, the feedback I get is maybe 5% of them were really concerned and didn’t know about it, and the other 95% don’t even respond. This has been my experience dealing with WMTS, which involves a federal regulation. How are we going to ensure adoption of IEC 80001, which is a voluntary standard?

**Mankovich:** Inside my company, there was actually some fear, uncertainty, and doubt. People not active with 80001’s development had the mistaken impression that it was a disruptive thing. Now, we’re starting to be asked about it by customers. In fact, just like with the early Health Insurance Portability and Accountability Act (HIPAA), we’re starting to get bids that say, “Please provide 80001-compliant equipment,” which, of course, makes no sense. I think it is very natural to see a bit of confusion at this early stage.

I have also seen more reasoned push-back. Before the standard was approved, some healthcare provider leaders in Germany and perhaps elsewhere said, “This sounds really nice and idealistic, but from my point of view, this is an unfunded mandate. I’m going to just push back as hard as I can.” There are others who won’t go near it because they are waiting until their funding organization, oftentimes the government, actually provides for staff funding to implement 80001. We may see resistance from providers who may not know the detail of the standard, but realize that this requires extra effort and they don’t have any extra people. We should anticipate that complaint.

**Grimes:** I frequently write and speak about the future of clinical engineering. Clinical engineering to this day in most organizations, certainly in the United States and arguably internationally as well, is focusing on things that often don’t significantly contribute to the reliability and effectiveness of today’s healthcare technology. When this profession got started in the early 1970s, its focus was on electrical safety. The Joint Commission mandated that electrical safety testing had to be completed four times a year on equipment. Fortunately, they’ve backed off on that requirement. Today, the problem is that to a significant degree, about 40% to 50% of what clinical engineering still does in hospitals is scheduled maintenance. The kinds of technologies we’re dealing with today don’t merit or benefit from that kind of service.

With 80001, we are talking about using risk and security management to redirect significant resources within the hospitals toward more effective support services. We need to point out to the clinical engineering community the importance of doing risk management, and how it enables us to identify and focus on those elements of support that have a potential of being a real benefit in improving the safety, effectiveness, and security of healthcare technology. I firmly believe this approach can be far more effective in improving technology safety and
effectiveness than some of these other things that clinical engineering is currently spending its time on.

In fact, if you do an effective risk management job, it’s going to get you focusing on where the real challenges are and what the real needs are. That may involve backing off on some of the scheduled maintenance where there’s no real merit in doing that kind of maintenance. But, that’s all going to come out in the risk management process.

Therefore, I’m not as concerned about there being the need for more clinical engineering resources. I think we’re really looking at just a different paradigm, a different approach, and that a lot of these resources just need to be re-directed in a more effective way.

Delvecchio: I think that reading the standard and having an understanding of the actual content inside the standard rather than just articles that have been written about it will help. I also think that the technical reports that are being developed will help a lot.

Eagles: Do healthcare providers expect medical manufacturers to be providing more information now that 80001 is published? And, if so, how do they engage the manufacturers who have not been involved in the standard’s development, who are as much in the dark as many of the hospitals are?

Grimes: It is not unprecedented for healthcare providers to ask for this kind of information. Back in 2003, under HIPAA, we were required to do risk management with respect to the security of our IT systems and medical devices that had protected health information. Suddenly, medical device manufacturers were being inundated with a variety of requests from 5,000 hospitals in almost as many different formats. Manufacturers were responding with their different information and different formats. It became extremely difficult to compare apples to apples with respect to the security assessment. That was the idea behind getting manufacturers and healthcare providers together to come up with the MDS² form,* which now provides the information in a standard way and allows people to do a consistent security assessment. The MDS² approach was very successful and got buy-in from all the major manufacturers. So, there is a precedent for requesting that kind of data in a way that was acceptable to both healthcare providers and most medical device manufacturers.

With respect to the information that manufacturers will provide to support 80001, it probably makes sense to take the same approach and ask an industry group or technical committee to develop a guideline, form, or standard way that this information can be collected, and a reasonable set of information that will be requested.

Martin Ellis: A slightly different approach might be required for IT vendors. As you know, they don’t operate within a regulated industry like medical device manufacturers do. I don’t know what sort of information IT vendors will have available to give health delivery organizations. The available data is going to vary from manufacturer to manufacturer, and it may not be readily available in the format that would be needed.

Getting all of the needed information is going to be a challenge for both the IT vendor industry and for the healthcare delivery organizations.

Doug Martin: As someone working for a healthcare provider organization wanting to buy a product, I would like to have a standardized questionnaire or dialog in the form of a document. I would send vendors an 80001 compliance document that asks key questions, like, “Do you do this? What happens when the device goes off the network? What are you doing for patching? What are you doing for virus protection?” The document would give the organization some space in the documentation to describe what they are doing for security.

Keep in mind that on the health delivery organization side, some organizations have network access con-

* The Manufacturer’s Disclosure Statement for Medical Device Security (MDS²) was originally developed by the Medical Device Security Workgroup of the Healthcare Information and Management Systems Society (HIMSS). MDS² was subsequently adopted by the National Electrical Manufacturers Association (NEMA) where it became a formal industry standard. The intent of the MDS² is to facilitate the consistent exchange of security related information between medical device manufacturers and healthcare providers in a manner that allowed those providers to effectively assess the vulnerability and risks associated with electronic Protected Health Information (ePHI) transmitted or maintained by medical devices.
trol packages that monitor threats, and some don't. Some have aggregation software that looks at all their virus protection and identifies infected devices, and some don't. Therefore, I don't think that one form is going to work for every organization.

Mankovich: This variability in health delivery organization network environments is one of the issues that we have to wrestle with as manufacturers. A medical device manufacturer operates under careful regulation with design controls and quality assurance requirements. Therefore, we typically build a single product for many, many customers. The business is structured to deliver a product in one form without a tremendous amount of individual product reengineering and customization according to different kinds of security environments. Customizing every product to every possible environment is not possible today. It may evolve that there are two or three different types of security environments that you, on the provider side, tell us you have and we may have to create product configuration options that will work in those environments.

But right now, if you started the ball rolling by giving me a very detailed disclosure about the security environment into which my product will have to fit, I wouldn’t be able to do much with that other than respond with the set of characteristics provided in my catalog product.

Of course, your security questionnaire would be the start of a dialog, but you will have to keep in mind that I’m not in a position to reengineer the product for you the same way you might, for example, change components of a car, like the fabric material on your car seats, paint color, tires, and the gear package. We’re just not set up as an industry to do that right now.

Martin: My interest is more knowing what am I getting into so that I can then make an informed decision. I wouldn’t ask a manufacturer or a vendor to change their process. I just want to understand what their process is.

Grimes: Within the NEMA MDS² Standard Revision Task Force, we are currently in the process of reviewing and considering an update of the MDS². The outcome of this review will likely result in the adoption of a new MDS² standard that incorporates at least key security information elements that healthcare providers will need from medical device manufacturers when those providers conduct their 80001 risk assessments. Given 80001’s focus on assessing risks associated with safety and efficacy as well as security, the Task Force is also considering whether it would be appropriate to broaden the information we ask manufacturers to provide in the MDS² to include material those manufacturers have on safety and efficacy that providers would find helpful when conducting their 80001 risk assessments.

Eagles: How might IEC 80001 affect the regulatory environment for medical devices?

Fitzgerald: One question is what effect a standard like 80001 might have on the premarket approval processes and the premarket evaluations in the United States and around the world. This is difficult to predict for a few reasons. The standard is about establishing a common semantic framework for transferring the right amount of risk management information across the barrier of commerce. It is very difficult to regulate that level of information. To the extent that it can be done without the regulator having to write down exactly what needs to be known, the better it is. Regulators don't know all that transpires inside the hospital environment that purchases these medical devices.

That being said, to the extent that a manufacturer is prepared to build a process for deliberately disclosing enough information to the widest possible customer base, that process would be of considerable interest during the premarket review process. And to the extent that such a declaration would be in some sense part of their labeling or their statements, that would also be of interest. Up
until now medical device regulators have not been rigorously asking for information about the cybersecurity aspects of medical devices.

I have a feeling, although I don’t know this, that as time moves forward that will change. It would be a useful thing at this moment for medical device manufacturers to begin to address the cybersecurity challenges that their devices may have when in the marketplace. 80001 provides them with a common semantic framework for establishing that level of information, and putting it all together in a package that the widest number of their customers can use.

There is going to be a learning period for both the medical device manufacturing community and the consumers of medical devices. They will both have to learn what is the right level of information.

There is another key question with regard to regulation. In many countries, the consumers of medical devices are government entities. To the extent that they are also the regulators of the hospital systems, they can in many cases command what those hospital systems buy and on what basis they buy them.

I imagine that the large purchasers of medical devices—be they governmental or private—may end up with a quasi-regulatory role. They are not just customers. They regulate the quality and the nature of the healthcare delivery system. And they’re increasingly becoming involved in the cyber-protection of the hospital systems that they own. I think you may see the advent of large-scale purchasing, particularly in European nationalized public trust hospitals. You may see those purchasers rise to the challenge of providing the resources in order to do this thing correctly as time moves forward.

We’re still very juvenile in the way that we think about incorporating medical devices into networks. I’m not sure that even the smartest of us—particularly those in the healthcare delivery arena—would pretend that this is a slam dunk and can be done overnight. The more pilots the better, in my opinion, and the lighter regulatory touch as we try to move this culture forward the better as well.

---

**Technical Reports Under Development**

Three new work item proposals that will provide additional guidance for implementing 80001 are out for vote. They are:

- IEC 80001-2-x, *Step by step risk management of medical IT-networks; practical applications and examples*
- IEC 80001-2-x, *Guidance for the communication of medical device security needs, risks and controls*
- IEC 80001-2-x, *Guidance for wireless networks*

If approved as new projects, these technical reports will likely be available in the fall of 2011.