AAMI
Advancing Safety in Healthcare Technology

Health IT Risk Management

A Practical Tool to Help Hospitals and Medical Devices Stay Secure in a Complex World

About this Report

This publication summarizes research and interviews with leading healthcare technology professionals around the United States. It is intended to be a helpful resource, and is not to be construed as an interpretation of AAMI standards, nor does it constitute legal or regulatory advice. We encourage you to share this publication with your colleagues. You may freely reproduce this publication, provided that proper attribution is made as follows: Copied with the permission of AAMI. This publication may not be sold in whole or in part.

Published by
AAMI
4301 N. Fairfax Drive, Suite 301
Arlington, Virginia 22203-1633
www.aami.org

Printed in the United States of America

ISBN 978-1-57020-649-8

> “Once you know the risks, you have to do something about it.”
>
> —Scot Copeland, clinical systems specialist
> at Scripps Health

Hospitals exist to help patients—to heal them, and to ease their suffering. But hospitals face new risks because of the highly technical and interconnected online world we live in. Consider these potentially disastrous, and highly plausible, scenarios: A seemingly harmless network upgrade causes the patient monitoring system in your pediatric intensive care unit (PICU) to fail. Or a routine software patch causes your entire fleet of infusion pumps to stop working simultaneously. Would your staff know what to do to keep your patients safe? Would your hospital continue to operate safely and effectively? Do you know how long it would take to recover?

Imagine having a plan in place that would help your staff know what to do under such alarming circumstances, *and* help prevent such disruptions from happening in the first place. Fortunately, a standard was developed by a distinguished committee of medical device manufacturers, information technology (IT) experts, and others with a keen understanding of medical devices and IT systems—and how they must work together. Their aim was to provide hospitals with detailed and practical guidance on how to operate a modern connected facility.

Voluntary, consensus standards are significant documents in healthcare technology, used by regulatory bodies such as the Food and Drug Administration (FDA) to support the development of safe and effective devices. In this case, the series of standards known by its shorthand—80001—provides a solid framework upon which to base a hospital’s approach to managing the ever-changing risks associated with healthcare IT networks. 80001 is applicable to every associated concern from the scores of individual medical devices found in hospitals to the complex system of systems that defines modern healthcare.

Why Pay Attention to the Risks?

As a senior executive, you're busy. You have plenty of priorities. But if you think health IT risk management is not worth your attention, think again. Health IT risks present significant *business* threats. Patient safety and satisfaction issues, downtime and inefficiencies, and data and system security problems can cost you—big time:

$2.2 million+

The average cost of a data breach in the healthcare industry

Poneman Institute, 2016[1]

$8,851 a minute, or $740,367 per incident

The average cost of unplanned data center downtime for healthcare organizations

Emerson Network Power, 2016[2]

82%

Health IT executives who report that their organizations are not prepared for security breaches, data loss, and unplanned outages

MeriTalk, 2014[3]

Top Business Risk: Reputation

Cyberthreats and data breaches can result in unflattering headlines, not to mention stiff fines from government regulators. These risks are increasing—and they are a rising concern for healthcare executives.

Allianz, 2016[4]; North Carolina State University's Enterprise Risk Management Initiative and Protiviti, 2016[5]; Deloitte, 2014[6]

Accreditation Concerns

Accrediting organizations such as The Joint Commission (TJC) have made it clear that they are paying attention to health IT issues.

Key Benefits of the 80001 Series

FOR RISK MANAGEMENT

- Provides a framework for analyzing and controlling health IT risks related to safety, effectiveness, and data and system security
- Helps mitigate constant cybersecurity threats with proactive risk control measures
- Improves change control processes, including upgrades, updates, software patches, and bugs remediation
- Identifies gaps in safety, effectiveness, and data and system security
- Ensures "ownership" for every component of systems and networks
- Supports comprehensive documentation of risk management activities
- Promotes shared responsibility and partnerships for the safety of health IT among healthcare systems and vendors

FOR ORGANIZATIONAL EFFECTIVENESS

- Facilitates organizational change to reflect the intersection of IT, clinical and biomedical engineering, and clinical practice
- Improves management of clinical systems and workflows
- Supports cross-departmental collaboration
- Reduces reactive labors and disaster-mode situations
- Instills proactive thinking and increases time for strategic planning
- Contributes to health IT uptime and staff productivity
- Supports effective procurement and onboarding of both medical and non-medical healthcare technology

FOR QUALITY IMPROVEMENTS

- Complements quality system implementation and improvements
- Increases use of best practices

FOR THE BOTTOM LINE

- Provides a framework for managing and obtaining total cost of ownership targets for the significant investment in health IT infrastructure and clinical mobility
- Helps reduce costs associated with downtime and inefficiencies

So you think you're ahead of the game …

- You've turned your healthcare system into a technological wonderland. ✓
- To stay on the leading edge, support clinical mobility, and strengthen community services, you're constantly integrating more innovative healthcare technology into enterprise systems. ✓
- You've built a crackerjack team of health IT, network, and wireless experts, even a dedicated security squad, to tend the whole shebang. ✓

So why are the people who know healthcare technology best still nervous? Simply put, they know from experience that there is inherent *risk* in your vast, connected health IT infrastructure.

More precisely, there's a triplet of key risks—and pain points—with health IT:

1. Safety. Clinicians will tell you what keeps them up at night: patient safety risks. Some of their biggest tech-related worries—such as loss of the communication lifeline for patients in transport—aren't even on the radar screen of health IT staff. (Want proof? See the case study, "Scripps Health Plugs Security Gaps in Telemetry with 80001," on page 11.)

Caregivers routinely encounter hiccups with medical devices and systems—and, sometimes, serious disruptions that can harm patients. Risk managers, quality managers, and biomedical and clinical engineers share this top concern.

2. Effectiveness. For your IT staff, health IT downtime is a key concern. Downtime compromises performance, reliability, and trust in healthcare technology—and results in inefficient operations. Network disruptions can hinder clinicians in accessing healthcare technology and information, which could lead to incorrect patient diagnosis, monitoring, or treatment, or failure to take timely action in patient care.[7]

Health IT is supposed to drive efficiencies. Too often, though, the many connected systems clinicians use daily don't play well together in the healthcare ecosystem or meet user needs. Burdensome—even chaotic—practices result, according to David Classen, chief medical information officer at Pascal Metrics and associate professor of medicine at the University of Utah.[8]

3. Data and system security. Cybersecurity risks are an escalating, top-of-mind concern for all health IT professionals—and for legal, compliance, and financial officers as well. Hackers make headlines by stealing or holding hostage digital records, including personal identifiable information. For example, clinical and administrative operations at hospitals in Washington, DC, and Maryland were crippled in March 2016 when hackers infiltrated MedStar Health networks, encrypted data, including electronic health records (EHRs), with a virus, and demanded a ransom payment.[9]

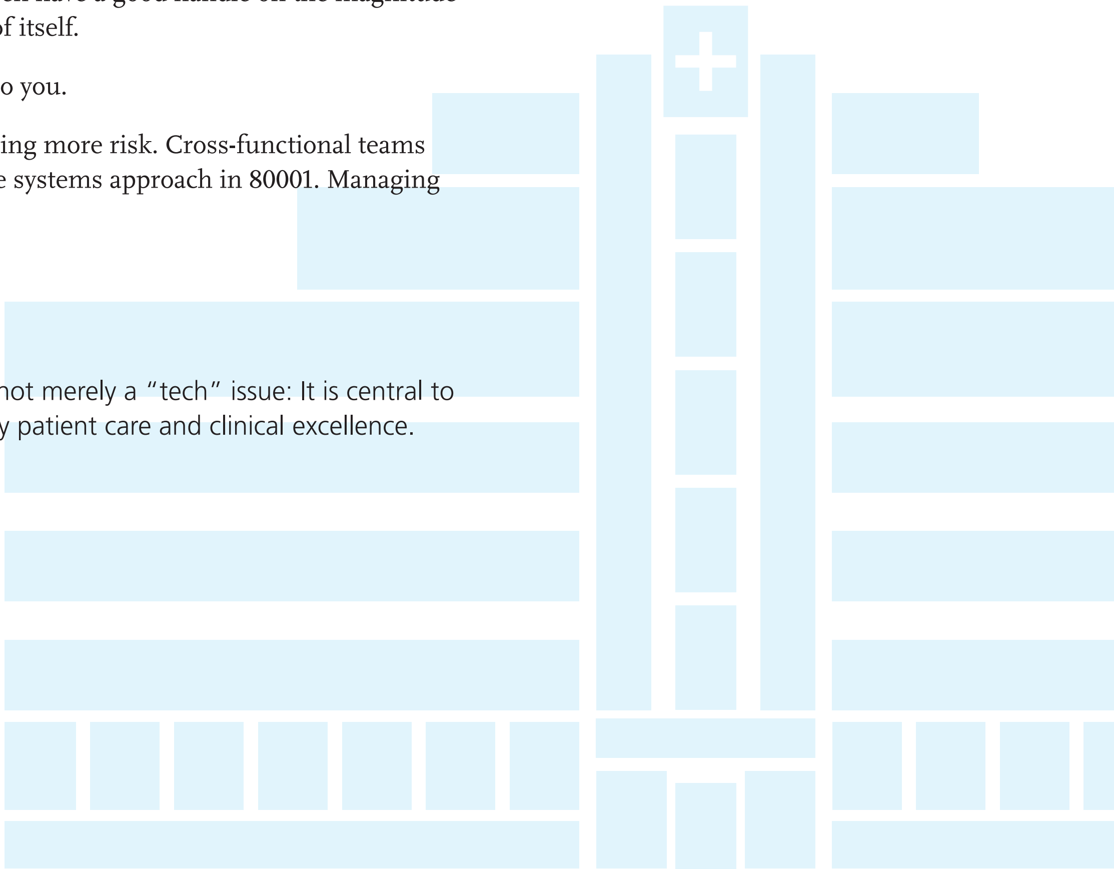
Silos in healthcare are creating more risk. Managing risk in silos will fail.

Malicious or inadvertent breaches aren't the only risks you face with data and system security. If healthcare technology, systems, and networks don't play well together, clinicians' access to vital patient data can be interrupted. Or that data might not flow seamlessly or accurately into EHRs—and that could impact not just patient care, but also reimbursement.

Admit it. Your healthcare system faces these risks every day. Worse, if your organization is like most, you don't even have a good handle on the magnitude of the risks—and that's a risk in and of itself.

What you don't know could catch up to you.

Moreover, silos in healthcare are creating more risk. Cross-functional teams need to own and manage risk with the systems approach in 80001. Managing risk in silos will fail.



KEY TAKEAWAY

Managing health IT risk is not merely a "tech" issue: It is central to your core mission of quality patient care and clinical excellence.

The time is right to leverage 80001—a standard tailor-made for managing *today's* health IT risks.

> "As health IT adoption spreads and becomes a critical component of organizational infrastructure, the potential for health IT-related harm will likely increase unless risk-reducing measures are put into place."
>
> —*Sentinel Event Alert 54*, The Joint Commission

Let's recap: You have risks—known and unknown—that could manifest into business challenges with significant consequences. What you most likely *don't* have is a systematic approach for managing the risks effectively. This is the missing piece in the health IT ecosystem that is leaving healthcare systems vulnerable and even holding back innovation.

This is where the 80001 series of standards* comes into play. 80001 defines the roles, responsibilities, and activities of healthcare delivery organizations in managing health IT risk. This includes refining or developing policies and procedures for identifying, assessing, and mitigating risks associated with key system properties—safety, effectiveness, and data and system security. (Yes, these key properties align with the triplet of major risks of health IT.)

To learn more about 80001, and find out how to order the standards from AAMI, see page 17.

Developers of the standards were ahead of the curve in anticipating the industry-wide shift from vendor-owned, proprietary medical IT networks to enterprise networks owned and managed by healthcare systems. This shift, spurred by quests for cost savings and in-house control, is well under way now.

In a sense, taking ownership of health IT is like buying a house: Both the benefits *and* the risks are all yours. You're responsible for the upkeep; you pay for asset meltdowns. Indeed, 80001 frames healthcare systems as "responsible organizations" for medical IT networks they own, whether they take a do-it-yourself approach or share responsibility for managing risk with vendors.

"A lot of mitigation work has to happen when you have ownership, so you don't just own it when it fails," said Scott Nudelman, general manager of biomedical services at GE Healthcare. "What do you do to prevent systems from failing? What are the processes you put in place? The healthcare industry just doesn't know where to go with all of this."

* ANSI/AAMI/IEC I 80001-1:2010, *Application of risk management for IT-networks incorporating medical devices.*

The Joint Commission (TJC) has taken notice of the shortcomings. In *Sentinel Event Alert 54* on the safe use of health IT, TJC in 2015 warned: “As health IT adoption spreads and becomes a critical component of organizational infrastructure, the potential for health IT-related harm will likely increase unless risk-reducing measures are put into place.”[10] The accreditation and certification organization referenced 80001 in recommending that healthcare systems improve risk management actions in three crucial areas:

1. **Safety culture**, including shared responsibility and involvement among healthcare organizations, clinicians, and vendors/developers
2. **Process improvement**, including developing a proactive, methodical approach to assessing patient safety risks and identifying system failures before they occur
3. **Leadership and oversight** of health IT planning, implementation, and evaluation

Clearly, satisfying the responsibility for health IT requires stronger, bolder action for mitigating risk. 80001 provides a road map and practical tools, which represent best practices, to do just that.

In fact, healthcare leaders who take a serious look at the standard recognize its value. “Whenever we present the standard to healthcare organizations, they say, ‘Yes, this is exactly what we need, this is exactly what we’ve been looking for,’” said Todd Cooper, executive director of Breakthrough Solutions Foundry and co-chair of the working group that drafted the standard.

> “What do you do to prevent systems from failing? What are the processes you put in place? The healthcare industry just doesn’t know where to go with all of this.”
>
> —Scott Nudelman, general manager of biomedical services at GE Healthcare

> “Whenever we present the standard to healthcare organizations, they say, ‘Yes, this is exactly what we need, this is exactly what we’ve been looking for.’ ”
>
> —Todd Cooper, executive director at Breakthrough Solutions Foundry and co-chair of ISO/TC 215

But wait—you already do risk management, right? Yes and no. You'd be surprised at what you're missing.

Clinical, biomedical engineering, and health IT leaders who ask senior executives to support an 80001 initiative in their healthcare systems often meet with a healthy skepticism. After all, cadres of people already manage health IT and address risk, right?

Yes and no. Healthcare systems that have the courage to take a systematic look at health IT risk come away astounded—and committed to act. The reason? They recognize striking gaps in responsibility for health IT and management of risk.

Take a patient monitoring system. Biomeds "own" the patient monitors and nurse or remote station monitors. IT staff own the enterprise network on which the monitors operate. "The IT department is really good at the enterprise network," said Nudelman, who works with hospitals in which GE Healthcare provides services to assess risk and improve value-based, care-driven technology. "They know exactly who owns it, whose job it is. There are regulatory bodies and OEM [original equipment manufacturer] specifications around how you manage your enterprise network. Biomeds know the segregated equipment."

Between the monitors and the network, however, is no man's land. A whole series of physical and virtual connections—cables, OEM switches, core switches, access switches to the EMR gateway, routers—serve as the glue that connects the monitors to the enterprise network. Data capture servers, application servers, interface engines, antennas, splitter boards, subsystems, and telecommunications switches can be in the mix of health IT connectivity as well.

Every networked system depends on these connections to work safety, effectively, and securely. In terms of responsibility, however, "there is a big cloud in the middle of all this integrated technology," Nudelman said. "If there's a problem with any of this equipment, these guys just point a finger at each other."

For an anesthesia system in one hospital, GE Healthcare identified 14 connections and interfaces to the enterprise network—out of sight in the walls, ceilings, and switch closets and out of mind in terms of both responsibility and even awareness. "That's 14 failure points you could have when the doctor says, 'My anesthesia machine is not reporting on the EMR,'" Nudelman said.

That's 14 potential failure points that no one owns—in just one system. Multiply that by the number of systems in a given organization or facility and the scope of unmanaged infrastructure and unmitigated risk becomes even more troubling. "You don't realize how bad it is until we do an actual gap analysis—and everybody's jaw is on the ground when they see the gaps," Nudelman added. "It's mind-blowing. Once you see it, you have to do something."

> “You don’t realize how bad it is until we do an actual gap analysis—and everybody’s jaw is on the ground when they see the gaps. It’s mind-blowing. Once you see it, you have to do something.”
>
> —Scott Nudelman, general manager of biomedical services at GE Healthcare

Scot Copeland of Scripps Health echoes that statement: “Once you know the risks, you have to do something about it.”

Figure 1 shows the gaps in responsibility that GE Healthcare discovered in one hospital’s health IT systems. The hospital then took action to close the gaps by clarifying who was responsible for every clinical device and system and every component of these systems.

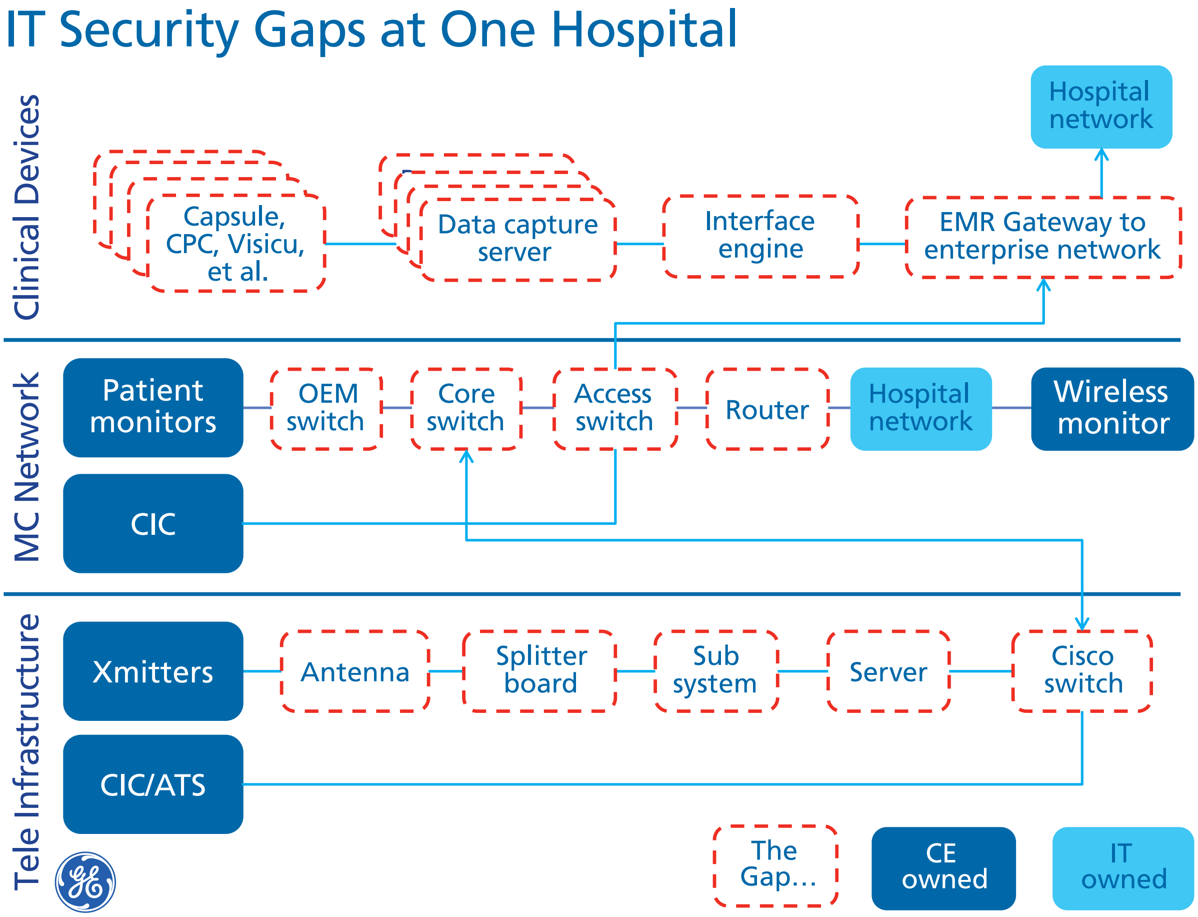


Figure 1. Minding the Gaps in Responsibility for Managing Risk

Source: The New Healthcare Technology World, GE Healthcare, May 2016. JB40441US. Used with permission.

“80001 covers all three key properties of medical devices on the health IT network—**safety, effectiveness, and security** of data and systems. It has something for everybody.”

—Scot Copeland, clinical systems specialist at Scripps Health

So yes, “you’re already doing risk management,” as Phil Raymond of Philips Healthcare tells healthcare system leaders and practitioners when he talks to them. “You’re already applying best practices,” to front-end devices and back-end enterprise networks. In many healthcare systems, this isn’t yet the case when it comes to the ever-expanding territory in the middle—the connectivity between devices and networks that’s a hallmark of the industrial Internet.

As far as the gaps go, “sticking your head in the sand and looking the other way is risk management,” Raymond said. “It’s poor risk management or it’s accepting a lot of risk, but you’re doing this already. 80001 is more about organizing and consciously applying risk management best practices.”

This is exactly what healthcare systems need now to manage health IT risk.

Tips for Getting Started and Staying the Course with 80001

Don’t take an “all or nothing” approach. 80001 has a couple of sticking points that give some healthcare system leaders pause: “First, the standard seems at first to entail a significant, systemic undertaking and considerable changes in practice, with no clear signals that current risk management methods are broken. Second, the standard requires healthcare delivery organizations to have a dedicated medical IT-network risk manager, which they are hesitant to do.”[11]

Doing something is better than doing nothing. And help is on the way: 80001 is in revision now—and one aim is to make the standard more user-friendly. In the meantime, ignoring risk is not a clever strategy. Here’s how to make the standard manageable and still achieve results, *starting now*:

- **Right-size your project.** Start with one critical, high-risk health IT system to learn the ropes.
- **Bring in third-party expertise and facilitation.** Experts in the 80001 standard and risk management can help educate staff, strengthen risk management skills, and keep your project on track.
- **Expand and sustain improvements and lessons learned.** Incorporate 80001 risk management into policies and procedures.

Scripps Health Plugs Security Gaps in Telemetry with 80001

> “We have been doing clinical risk management for 20 years. But 80001 is a more industrial-strength version of risk management for systems, software, and networks.”
>
> —Marcia Wylie, senior director of biomedical engineering at Scripps Health

The Biomedical Engineering Department of Scripps Health, based in San Diego, CA, had had its eye on 80001 for a year or two, and talked it up with administrators, before it found an opportunity to put it to the test. The proving ground: a brand new hospital, where a brand new wireless telemetry system would be installed on a brand new, enterprise-wide wireless network.

“We were nervous about putting our telemetry system on the Scripps house-wide wireless network,” said Marcia Wylie, senior director of biomedical engineering at Scripps Health. “For us, it was about patient safety and effectiveness. We were afraid—what happens when they do a change and it affects telemetry for 300 patients? Telemetry is a poster child.”

Data and system security was the driving force behind interest in 80001 for IT, IS [information services], and security staff. “The IT Department realized they were missing medical devices as they tried to get their hands around security,” Wylie said. “This came at the right time for them to include medical devices in that whole area.”

Managing security risks also appealed to the vice president of compliance, who is responsible for security audits and who endorsed the project, as well as the Scripps general counsel. Getting that leadership endorsement was important, given that the standard engages key stakeholders to capture broad perspectives on risk management.

> Managing security risks appealed to the vice president of compliance, who is responsible for security audits and who endorsed the project, as well as the Scripps general counsel.

Besides this perfect test case, the project came together when the Center for Medical Interoperability (C4MI) offered technical assistance with 80001 initiatives to member healthcare organizations. C4MI facilitated a four-stage process to implement the standard:

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

In Phase 1, C4MI used 80001 tools to probe stakeholders in depth about policies and procedures already in place for managing risk, such as change control responsibilities and processes, and the potential impact on patient safety and clinical practice. Out of that process came 15 recommendations, listed on page 13, which became action items for managing risk across the healthcare system’s health IT portfolio.

“We discovered that we were not starting from zero,” Wylie said. “We had a lot of policies, processes, and procedures in place already. We just needed to tie them together.”

Added Scot Copeland, clinical systems specialist at Scripps Health: “We modified about half a dozen policies we already had in place to include 80001. We put them into a framework that would address the three key properties of safety, effectiveness, and data and system security.

Basically, we folded medical device security and functions into existing IT security processes."

A C4MI contractor who is well versed in risk management tools worked part-time with the Scripps team for about six months on the project. To facilitate collaboration, document management, and risk management, she helped the team create a SharePoint website that serves as a "live risk register," with risk management policies, procedures, and forms and a repository for change permits, among other tools now centrally located and accessible.

At the same time, the Phase 1 readiness assessment and Phase 2 targeted risk assessment of the telemetry system did reveal gaps in risk management. "One of the values of the process, and something that we didn't foresee, was that clinicians were already concerned about risk," Copeland said. "It was because of the way the technologies go together and the way they actually used them in the environment."

A case in point: "When we asked what scared them the most about the telemetry system, they said, 'the portable phones,'" Copeland continued. "Pause for effect there, because everybody thinks, 'What do portable phones have to do with telemetry?'"

It turns out that the hospital had spotty phone coverage. When transporting a patient who needed to be monitored all the time, nurses would intermittently lose communication. They asked tough questions, Copeland said: "What happened if they were in an elevator and a patient coded or something? Could they get in touch with the code team or the people they needed to do a proper response to that situation? Or would they even know about the situation, if the teletech saw an arrhythmia during transport and couldn't reach the person who was responsible for escorting the patient? What would they do? That was the big thing that bugged clinicians and we hadn't even thought of that."

The Scripps team investigated this issue further—and discovered that there was no standard, no policy, no documentation, and no training for teletechs or anyone else for a situation like this. "That was an issue right there," Copeland said. "We found out it wasn't just the telesystem, it was system-wide. That was a big find. That was worth the price of admission for me right there." Since then, nurse executives have been working to address this issue.

In addition to assessing readiness and risks in Phases 1 and 2, Scripps and C4MI also provided training in 80001 risk management during stakeholder meetings. A reassessment of key stakeholders—including biomedical, IT, and IS staff—in Phase 3 resulted in a 3X improvement in knowledge.

> "When we asked what scared them the most about the telemetry system, they said, 'the portable phones."
>
> —Scot Copeland, clinical systems specialist at Scripps Health

In Phase 4, Scripps solidified its risk management practices by applying 80001 to a physiological monitoring system in a post-anesthesia care unit in a different hospital. This project, completed without C4MI's assistance, resulted in a risk management plan for that system.

The value of 80001, and lessons learned, for Scripps Health. Implementing the standard did what it was supposed to do for Scripps Health—identify and address risks and safety gaps in two critical health IT systems. So what's changed at Scripps? What are the lessons learned?

1. **80001 brings robust, "industrial-strength" risk management tools and processes to healthcare systems.** "We've been doing clinical risk management for 20 years," Wylie said. "But 80001 is a more industrial-strength version of risk management for systems, software, and networks." 80001 tools yield a more sophisticated risk analysis, based on probability and severity of risk, and a "manufacturer version" of risk management that takes into account system design.

2. **Leveraging in-house skills with third-party expertise and facilitation is an excellent model for implementing 80001.** C4MI's knowledge of the standard expedited the learning curve on the unfamiliar processes and tools for the Scripps team. Just as important, C4MI educated Scripps leadership on the value of the standard—and facilitated the fact-finding sessions. Sometimes, these meetings can be uncomfortable, particularly when safety gaps are exposed. An outsider with no skin in the game can keep these meetings productive.

3. **Targeting one critical health IT system is a good entry point to 80001.** Rather than trying to implement system-wide right off the bat, starting with the telemetry system proved to be a manageable project for Scripps. The benefits and lessons learned about the process from a discrete system carry forward to future projects.

4. **80001 instills a proactive, collaborative approach to risk management.** The biomedical, IT, clinical, and risk management departments now work together not just on risk management, but also on cross-functional due diligence and technical review of health IT before it comes in the door.

5. **By building awareness and distributing responsibility for risk management, 80001 calms nerves.** "The whole topic of risk management has gained visibility, so people pay attention to it more," Wylie said. "The awareness and nervousness is shared amongst others now, not just us. Things can still happen, but we are in a much better position now to proactively get in front of them."

6. **80001 supports partnerships with vendors.** "We never really involved the device manufacturers in our risk management conversations before," Wylie said. That's changing—and Scripps is finding that sharing the common language of 80001 with vendors is helpful.

7. **80001 principles and tools can be useful for managing risk of systems beyond health IT.** Scripps is now planning to apply 80001 processes not just to health IT, but also to facilities operations and physical security, such as HVAC and security systems and equipment. Some of those systems are clinically vital, such as medical air that keeps operating rooms at the right temperature.

OUTCOMES OF THE 80001 PROCESS

Scripps Health's 15 Action Items for Improving Risk Management

1. Create a Medical IT Network Risk Manager position.

2. Broaden the IT Risk Management Team to include IT, IS, clinical, biomedical, and audit and compliance. Add the Medical IT Network Risk Manager to the core IT Risk Management Team.

3. Include the three key properties of the medical IT network (safety, effectiveness, security of data/systems) in the risk management policy.

4. Add a risk/benefit analysis of residual risk that is signed off by the Medical IT Network Risk Manager and top management.

5. Change the process so that every change to the medical IT network requires a risk management project or a change permit, if one already exists. If one does not exist for the requested change, a risk management project is launched and the outcome of that project is either an authorized change, a change permit for a well-defined group of similar changes, or a rejection of the proposed change pending additional risk control measures.

6. Require go-live for all medical IT-network implementations to be authorized by the Medical IT Network Risk Manager.

7. Provide the Medical IT Network Risk Manager access to the current network configuration and to the list of devices on the medical IT network.

8. Document risk management discussions as a hazards analysis with risk assessment, identification of risk control measures, and evaluation of residual risk.

9. Add a process to prioritize, track, and measure effectiveness of risk control measures.

10. Define it to be the role of the Medical IT Network Risk Manager to manage medical device manufacturer (MDM) and Medical IT network component (NCM) vendors' risk management responsibilities.

11. Define it to be the role of the Medical IT Network Risk Manager to manage the risk management-related communications between the organization and vendors (MDMs and NCMs) with whom there is a risk management responsibility agreement related to the medical IT-network.

12. Create a central repository for all medical IT network risk management information.

13. Define it to be the role of the Medical IT Network Risk Manager to ensure that all medical IT network CAPAs [corrective and preventive actions] are closed in a timely manner.

14. Use a tool for traceability of identified risk control measures.

15. Focus the risk management policy on the particular medical IT network that it governs.

An attractive bonus: 80001 positions healthcare systems to realize efficiencies and cost savings from the Industrial Internet.

Beyond answering the need for more effective risk management, 80001 also can help healthcare systems improve health IT management and practices—and achieve business results.

“I think we’re right at the crux of hospitals really understanding that we are in the middle of what GE and the rest of the world call the ‘Industrial Internet,’” Nudelman said. The Industrial Internet brings together “brilliant machines, advanced analytics, and people at work,”[12] in GE’s words, to improve performance, uptime, and productivity.

In healthcare, intelligent, networked health IT, which includes the Internet of Things (IoT), provides real-time monitoring and diagnostics for operational intelligence, including asset life-cycle management and predictions about what will happen next, enabling people to make their best decisions.[13, 14]

DATA POINTS

“Clinical and operations inefficiencies, which can be most directly impacted by the Industrial Internet, account for **59 percent** of healthcare inefficiencies representing **$429 billion** per year. It is estimated that deployment of the Industrial Internet can help to drive these costs down roughly **25 percent**, or about **$100 billion** per year in savings. In this case, a one percent reduction in costs translates to **$4.2 billion** per year—or **$63 billion over 15 years**.”[15]

“If you want to be part of the Industrial Internet, you need to change the way you work,” Nudelman said. “Fixing broken things is not the future. Think about a pulse oximeter that used to be a whole device with a cable and finger probe. That eventually became a circuit board inside another device. That pulse oximeter is now a Bluetooth finger probe. It’s disposable.”

Given the built-in diagnostics and remote repair and upgrade capability of today’s healthcare technology, plus the trend toward more disposable products, the break–fix service model of clinical and biomedical engineering is fast becoming obsolete. The “CE–IT convergence,” insider shorthand for the overlap of clinical engineering and IT roles and responsibilities, reflects these changes.

Today's environment demands improved management of healthcare technology, systems, and networks—the infrastructure of the Industrial Internet—including risk. Improving safety, effectiveness, and data and system security will help healthcare systems maximize the potential benefits of the industrial Internet.

With more and more health IT integrated in myriad combinations, managing risk is becoming more complicated by the day. Nudelman speaks from experience on this point. GE Healthcare supports some 700 hospitals in managing their medical technology. "In my world, I have 89,000 unique make–model combinations," he said. "I have 3 million devices in my CMMS [computerized maintenance management system] today. I see 160 new configurations of makes and models every month.

"If you ask the end user, what's your biggest problem with biomed or HTM today, they say, 'how my integrated devices talk to the network," Nudelman added. "The infusion pumps that are supposed to get the drug libraries automatically through the Wi-Fi, they're never connecting. There's always a problem. Who do you call?"

Every health IT integration has its own risk profile. Every healthcare system has dozens or more systems in its technology portfolio. "As the complexity of systems increase, the time for adoption of 80001 is right," said Raymond, who directs the Wireless Competency Center at Philips Healthcare.

For the Industrial Internet to really take off, interoperability of connected health IT is crucial. "Executives get excited about driving true interoperability because they keep getting stuck with systems that they're told are interoperable and they're not," said Cooper. "Then they have to spend millions of dollars just patching together something that is brittle—and they're not getting the benefits that they want. Essentially, they want to solve the problem from a technical standpoint."

This scenario is especially familiar with electronic medical record [EMR] systems. Rather than approaching this challenge from a purely technical standpoint, a broader risk management perspective would yield a better solution. "How do you not only get interoperable technologies, but then leverage the implementation, use, and management of those technologies to where you engender trust on the part of all stakeholders?" Cooper asked. "My definition of trust is establishing a high level of confidence on the part of all stakeholders that their interoperable technologies will perform as expected safety and securely. That's where 80001 comes in."

80001 Helps to Bridge the "People–Process Gap" in Risk Management

Even with the best intentions, people are limited in their knowledge of different types of risk by their particular areas of expertise:

- HTM professionals tend to focus on patient safety, management of medical devices on wired and wireless networks, and the effectiveness of healthcare technology.
- IT, network, wireless, and security professionals tend to focus on data and system security, downtime, and change control processes.
- Other healthcare professionals are most concerned about clinical practice and workflow, quality, liability, or finances.

These points of view are valuable, but there's no mechanism for putting them all together into a comprehensive picture of risk.

Often, these professionals work largely in silos, so they don't have much opportunity to build a collective understanding of health IT risk. Even in healthcare systems where IT and clinical or biomedical engineering staff work well together, responsibility for managing risk can be ill defined and, sometimes, contentious. Everybody's busy and staffing is tight.

80001 provides a framework, processes, and tools to help bridge the "people–process gap" constructively and collaboratively.

AAMI/FDA Summit Results in Action Plan for Improving Risk Management

Healthcare systems are not alone in their need for better ways to manage health IT risk. As healthcare technology proliferates and becomes more complex, all stakeholders are experiencing similar pressures.

In 2015, AAMI and the FDA convened a Risk Management Summit to put the issues in the spotlight. The summit made clear that everyone who is involved with healthcare technology can and should contribute to risk management.

More than 200 participants from industry, healthcare systems, and professional and regulatory organizations advocated for a full life-cycle approach to managing health IT risks. For healthcare systems, for example, they recommended broader "ownership" of risk management to include the untapped expertise of people who know healthcare technology best, especially clinicians.

The summit resulted in five "**clarion themes**"[16] to be used as an action plan to help the healthcare community better manage health IT risk and improve patient safety:

1. Recognize that everyone in healthcare is a risk manager.
2. Develop shared understandings of the risks—and benefits—of healthcare technology.
3. Adapt systems engineering principles, practices, and tools for risk management.
4. Engage in a total life cycle approach to risk management of healthcare. technology, which is required for *effectively* managing risk.
5. Create new practical tools to continue advancing the field of risk management for healthcare technology.

What Does 80001 Cover?

Recognizing that medical devices are incorporated into IT networks to achieve desirable benefits (for example, interoperability), this international standard defines the roles, responsibilities and activities that are necessary for risk management of IT networks incorporating medical devices to address **safety**, **effectiveness**, and **data and system security**.

ISO/TC 215, *Health informatics*, and IEC/SC 62A, *Common aspects of electrical equipment used in medical practice*, developed the 80001 series of standards and technical reports. The series covers roles, responsibilities, and activities for organizations and key individuals in managing risk:

- Responsible organizations
- Top management
- Medical IT network risk manager
- Medical device manufacturer(s)
- Providers of other information technology

The series covers the activities and documentation required for effective risk management throughout the full life cycle of health IT. Annexes to the standard explain its rationale, provide an overview of risk management relationships, provide guidance on how to use it, and describe its relationship to other standards.

TO ORDER, CONTACT AAMI

AAMI, which administers the international work on this series (on behalf of ANSI), has adopted all the existing parts of the existing 80001 series as American National Standards or as AAMI Technical Information Reports.

These reports can be purchased at **www.aami.org/store** or by calling +1-877-249-8226.

Published Parts of the 80001 Series

- IEC 80001-1:2010, *Application of risk management for IT-networks incorporating medical devices—Part 1: Roles, responsibilities and activities*
- IEC/TR 80001-2-1:2012, *Application of risk management for IT-networks incorporating medical devices—Part 2-1: Step by Step Risk Management of Medical IT-Networks; Practical Applications and Examples* (adopted by AAMI as ANSI/AAMI/ISO TIR80001-2-1:2012)
- IEC/TR 80001-2-2:2012, *Application of risk management for IT-networks incorporating medical devices—Part 2-2: Guidance for the communication of medical device security needs, risks and controls*
- IEC 80001-2-3:2012, *Application of risk management for IT-networks incorporating medical devices—Part 2-3: Guidance for wireless networks*
- IEC/TR 80001-2-4:2012, *Application of risk management for IT-networks incorporating medical devices—Part 2-4: General implementation guidance for Healthcare Delivery Organizations*
- IEC/TR 80001-2-5:2014, *Application of risk management for IT-networks incorporating medical devices—Part 2-5: Application guidance—Guidance for distributed alarm systems*
- ISO/TR 80001-2-6:2014, *Application of risk management for IT-networks incorporating medical devices—Part 2-6: Application guidance—Guidance for responsibility agreements*
- ISO/TR 80001-2-7:2015, *Application of risk management for IT-networks incorporating medical devices—Application guidance—Part 2-7: Guidance for healthcare delivery organizations (HDOs) on how to self-assess their conformance with IEC 80001-1*
- IEC/TR 80001-2-8:2016, *Application of risk management for IT-networks incorporating medical devices—Part 2-8: Application guidance—Guidance on standards for establishing the security capabilities identified in IEC 80001-2-2*
- IEC/DTR 80001-2-9:2017, *Application of risk management for IT-networks incorporating medical devices—Part 2-9: Application guidance—Guidance for use of security assurance cases to demonstrate confidence in IEC/TR 80001-2-2 security capabilities*

AAMI has adopted all parts of the 80001 series as American National Standards or AAMI Technical Information Reports.

References

1. **Ponemon Institute.** (May 2016). Sixth annual benchmark study on privacy & security of healthcare data. Available at www.ponemon.org/blog/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data. Accessed Sept. 2, 2016.

2. **Emerson Network Power.** (Jan. 19, 2016). Emerson Network Power study says unplanned data center outages cost companies nearly $9,000 per minute. Press release. Available at www.emersonnetworkpower.com/en-US/About/NewsRoom/NewsReleases/Pages/Emerson-Network-Power-Study-Says-Unplanned-Data-Center-Outages-Cost-Companies-Nearly-9000-Per-Minute-.aspx. Accessed July 22, 2016.

3. **MeriTalk.** (Feb. 3, 2014). 82 percent of health IT executives report their organizations are not prepared for the unexpected. Press release. Available at www.meritalk.com/wp-content/uploads/2015/12/MeriTalk_Rx_ITaaS_Release.pdf. Accessed July 22, 2016.

4. **Allianz.** (2016. Allianz risk barometer: Top business risks 2016. Available at www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf. Accessed July 22, 2016.

5. **North Carolina State University's Enterprise Risk Management Initiative and Protiviti.** (2016). Executive perspectives on top risks for 2016: Key issues being discussed in the boardroom and C-suite. Available at www.protiviti.com/en-US/Documents/Surveys/NC-State-Protiviti-Survey-Top-Risks-2016.pdf. Accessed July 22, 2016.

6. **Deloitte.** (October 2014). 2014 global survey on reputation risk. Available at www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_Reputation_Risk_survey_EN.pdf. Accessed July 22, 2016.

7. **Cooper T, David Y, Eagles S.** (2011). *Getting Started with IEC 80001: Essential Information for Healthcare Providers Managing Medical IT-Networks*. Association for the Advancement of Medical Instrumentation.

8. **Association for the Advancement of Medical Instrumentation.** (November 2015). Toward a shared responsibility for health IT safety: Standards for quality management and risk management processes for health IT. AAMI stakeholder workshop summary report.

9. **Duncan I, McDaniels AK.** (April 2, 2016). MedStar hack shows risk that comes with electronic health records. *The Baltimore Sun*. Available at www.baltimoresun.com/health/bs-md-medstar-healthcare-hack-20160402-story.html. Accessed April 8, 2016.

10. **The Joint Commission.** Sentinel Event Alert 54. (March 31, 2015). Available at www.jointcommission.org/assets/1/18/SEA_54.pdf. Accessed Feb. 13, 2016.

11. **Vockley M.** (March/April 2016). Making wireless work: A look at what hospitals are doing. *Biomedical Instrumentation & Technology*: Vol. 50, No. 2, pp. 92–101. Available at www.aami.org/making_wireless_work.

12. **GE.** The industrial internet. Available at www.ge.com/digital/industrial-internet. Accessed Feb. 10, 2016.

13. **GE Healthcare.** Centricity solutions for integrated care. Available at www.ge.com/industries/healthcare/. Accessed Feb. 10, 2016.

14. **GE.** How does the industrial internet of things work? Available at www.ge.com/digital/blog/How-does-the-Industrial-Internet-Work. Accessed Feb. 10, 2016.

15. **Evans PC, Annunziata M.** (Nov. 26, 2012). Industrial internet: Pushing the boundaries on minds and machines. GE. Available at www.ge.com/docs/chapters/Industrial_Internet.pdf. Accessed Feb. 10, 2016.

16. **Vockley M.** (2015). Making risk management everybody's business. Association for the Advancement of Medical Instrumentation. Available at www.aami.org/Risk_Management_Summit_Report.pdf. Accessed Feb. 17, 2016.

Acknowledgments

AAMI would like to thank the thought leaders who helped shape this publication, the contributors who shared their stories, and the reviewers who strengthened the final outcome.

A special word of thanks to **Martha Vockley**, an AAMI freelance writer; and **Ruth Moyer**, a freelance graphic designer who managed the project.

This publication wouldn't have been possible without the help of attendees from the AAMI Stakeholder Workshop on Standards for Quality Management and Risk Management Processes for Health Information Technology (IT) and numerous other AAMI volunteers who helped develop and review content.

A special thanks to these individuals:

Contributors and Reviewers

Todd Cooper
Executive Director
Breakthrough Solutions Foundry
Co-chair of ISO/TC 215

Scot Copeland
Clinical Systems Specialist
Scripps Health

Kathy Kenyon
Health policy, law, and compliance consultant

Kenneth Maddock
BI&T Editorial Board Member

Scott Nudelman
General Manager of Biomedical Services
GE Healthcare

Phil Raymond
Director of the Wireless Competency Center
Philips Healthcare

Marcia Wylie
Senior Director of Biomedical Engineering
Scripps Health

AAMI Staff

Steve Campbell
Chief Operating Officer

Joe Lewelling
Vice President of Emerging Technologies and Health IT

Patrick Bernat
Director of Healthcare Technology Management

Mary Logan
Former President

Sean Loughlin
Vice President of Communications

Barbara Saxton
Website Director

AAMI
Advancing Safety in Healthcare Technology

4301 N. Fairfax Drive, Suite 301 Arlington, VA 22203-1633 +1-703-525-4890 www.aami.org