Networked Medical Devices: Essential Collaboration for Improved Safety

Steven R. Rakitin

A recent Sentinel Event Alert published by the Joint Commission stated:

> *As health information technology (HIT) and "converging technologies"—the interrelationship between medical devices and HIT—are increasingly adopted by healthcare organizations, users must be mindful of the safety risks and preventable adverse events that these implementations can create or perpetuate. Technology-related adverse events can be associated with all components of a comprehensive technology system and may involve errors of either commission or omission. These unintended adverse events typically stem from human/machine interfaces or organization/system design. The overall safety and effectiveness of technology in healthcare ultimately depend on human users ideally working in close concert with properly designed and installed electronic systems. Any form of technology may adversely affect the quality and safety of care if it is designed or implemented improperly or is misinterpreted. Not only must the technology or device be designed to be safe, it must also be operated safely within a safe workflow process.*[1]

The "converging technologies" referred to by the Joint Commission are predominately software-based medical devices that are increasingly being connected to networks within healthcare organizations. Medical devices must be safe and effective when connected to a healthcare organization's network. And, in the not-too-distant future, medical devices may interoperate in ways we have yet to define. The interoperability spectrum includes everything from sharing of clinical information to allowing medical devices to control other medical devices.

A recent report on integrating technology into the healthcare environment by the Committee on Engaging the Computer Science Research Community in Healthcare Informatics of the National Research Council found that:

> *"... the acquisition processes of many healthcare provider organizations are not often compatible with the development and deployment of future healthcare IT systems that provide cognitive support and are evolvable into the future. Poorly understood or defined requirements, poor development processes, and failure to adopt iterative or evolutionary approaches or user-centered design are often seen."*[2]

The days of standalone medical devices that can be easily validated by referring to service manuals are long gone. Today, validating complex medical devices used in a variety of healthcare network environments that often include other medical devices, as well as nonmedical equipment (such as routers and servers) and software, is a daunting task. Even more daunting is the task of performing risk management for these complex medical devices when they are connected to different healthcare network environments. Ill-defined roles and responsibilities of medical device manufacturers and the healthcare organization's clinical engineering-information technology (CE-IT) staff with respect to risk management and validation further complicates the situation. In a recent article on patient safety in networked healthcare systems, Sherman Eagles stated:

> *Complex networked systems, including medical devices, have now become common, and with this added sophistication, new behaviors and unexpected consequences have begun to appear that are outside the control of the medical device manufacturer.*[3]

Design validation and risk management are examples of required activities performed by medical device manufacturers to help ensure that devices are as safe as "reasonably practical." While design validation and risk

Author's note: The draft standard IEC/CD2 80001—Application of risk management for IT networks incorporating medical devices *(Nov. 21, 2008) has not been released to the public. Therefore material cited here is paraphrased rather than quoted directly.*

management have improved the safety of medical devices, the effectiveness of these activities is directly related to the ability of the device manufacturer to understand and simulate the disparate networking environments within which these medical devices are used. Increasing the effectiveness of design validation and risk management in complex networking environments will require the full cooperation and active participation of stakeholders, including medical device manufacturers, IT network equipment suppliers, clinical and biomedical engineers, and IT staff, as well as regulators.

The Joint Commission Sentinel Event Alert raises two important questions:

1. What are stakeholders currently doing to ensure that networked medical devices are as safe as "reasonably practical"?
2. What additional steps can stakeholders take to ensure that networked medical devices of the future are safer than they are today?

There are several safeguards presently in place to ensure the safety and efficacy of medical devices. These safeguards include the U.S. Food and Drug Administration's (FDA) Pre-market Review Process and required tasks such as design review, design validation, software validation, and risk assessment.

FDA Pre-market Review Process

FDA's pre-market review process requires most medical device manufacturers to submit information (commonly referred to as a 510k) about the medical device to FDA before the device can be legally marketed in the United States. Some low-risk medical devices are exempt from the 510k requirement and other higher-risk devices require a much more extensive Pre-market Approval (referred to as a PMA).

A 510k requires demonstration of *substantial equivalence* to another legally U.S.-marketed device called the *predicate*. Substantial equivalence means that FDA has determined that the new medical device is at least as safe and effective as the predicate, based upon a review of documentation and performance data included in the 510k. A medical device may not be legally marketed in the United States until the device manufacturer receives written approval from FDA declaring the new medical device *substantially equivalent*.

A device is *substantially equivalent* if, in comparison to the predicate device, it has the same intended use and the same technological characteristics; or it has the same intended use as the predicate and has different technological characteristics and the information submitted to FDA does not raise new questions of safety and effectiveness and the information demonstrates that the device is at least as safe and effective as the legally marketed predicate device

A potential concern with the 510k model is that predicate devices may be several years old and, as a result, may not have been designed to be networked. The technological characteristics referred to in determining substantial equivalence often are directly related to intended use and may not include network connectivity.

Design Review, Design Validation, and Software Validation

Medical device manufacturers are required to perform design review and validation as part of the medical device development process as defined in the Quality System Regulation. Design reviews—systematic peer reviews of various aspects of the medical device development process—are planned and often include reviews of requirements, system and software design, and code. As stated in the FDA Quality System Regulation, design validation "shall ensure that devices conform to defined user needs and intended uses and shall include testing of production units under actual or simulated use conditions."[4]

FDA's General Principles of Software Validation Guidance defines software validation as "confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled."[5] Additionally, the guidance states that "...testing at the user site is an essential part of software validation" and that "this testing should take place at a user's site with the actual hardware and software that will be part of the installed system configuration."

Among the many challenges facing device manufacturers is performing design validation "...under actual or simulated use conditions." When "actual use conditions" include connecting medical devices to a healthcare organization's network, device manufacturers must somehow address the fact that every healthcare organization's network is different. The safety and efficacy of medical devices can often be affected by the network the device is connected to. Some device manufacturers perform design validation activities with their medical devices connected to the healthcare organization's network. However, the

Healthcare organization policies regarding installing of unapproved or unreleased devices on their network differ widely from one organization to another.
The roles and responsibilities of the device manufacturer and the healthcare organization's CE-IT staff are not clearly defined with respect to design validation and risk management.
Medical device manufacturers are reluctant to share technical information about their medical devices with CE-IT staff.
Device manufacturers may not be fully aware of the different clinical use cases and workflows that include their medical devices that are used within each healthcare organization.

Table 1. Factors affecting the effectiveness of design validation activities performed by device manufacturers.

results of this activity can be limited and incomplete for the reasons shown in Table 1.

In addition to design validation activities performed by device manufacturers, CEs often create validation protocols as an acceptance test when integrating newly acquired devices into their environment. The effectiveness of these validation protocols is limited by the lack of technical information from the device manufacturers.

Risk Management

ANSI/AAMI/ISO 14971:2007—*Medical devices—Application of risk management to medical devices*, defines requirements for performing a risk assessment of medical devices. A key requirement of this standard states that:

> *"For the particular medical device being considered, the manufacturer shall document the intended use and reasonably foreseeable misuse. The manufacturer shall identify and document those qualitative and quantitative characteristics that could affect the safety of the medical device and, where appropriate, their defined limits."*[6]

Every healthcare organization's network is unique. Further, clinicians who use networked medical devices may use them in ways that are specific to that institution. The challenge facing the healthcare community is how to identify risks associated with using medical devices in each and every situation. If a healthcare organization chooses to connect a medical device to a network in a manner that was not tested or even considered by the medical device manufacturer, does this constitute what ANSI/AAMI/ISO 14971 calls "reasonably foreseeable misuse?"

Medical device manufacturers may not support connecting their medical devices to networks in the healthcare environment.
The medical device may not operate properly when connected to a network containing other medical devices and other equipment.
Medical device software may not operate correctly as a result of other software applications running on the same network.
Conflicts may arise between the need to control changes to medical devices and the constant need to upgrade antivirus software to protect against cyber attacks.

Table 2. Potential problems associated with incorporating medical devices into IT networks (*based on examples presented in 80001 draft*).

Additional Steps

The November 2008 draft of the forthcoming standard IEC/CD2 80001—*Application of risk management for IT-networks incorporating medical devices* identifies a number of potential problems associated with the incorporation of medical devices into IT networks. Examples of these problems are listed in Table 2.

Increase Collaboration and Sharing of Critical Information

Presently, there is far too little collaboration and sharing of information between the stakeholders. For example, medical device manufacturers share little, if any, information about the risk management and design validation tasks performed for a medical device. The healthcare organization's CE-IT staff is often protective of critical networking information. The CEs may not be privy to relevant information regarding the network configuration and the IT staff may not be knowledgeable in how networked medical devices are affected by changes to the network. Clinicians may not be aware of how medical devices behave when networked.

What's needed is a much more open and collaborative relationship between all of the stakeholders: medical device manufacturers, IT network suppliers, the healthcare organization's CE and IT staffs, clinicians, and regulators. In order for the stakeholders to collaborate more effectively, there needs to be a common language that is used and understood. For example, all of the stakeholders need a common understanding of terms such as "reasonably foreseeable misuse" and "actual use conditions." Without a common language, increased collaboration will not be possible.

Medical device manufacturers develop medical devices

for a wide variety of customers (healthcare organizations). Manufacturers need to be aware of the many different "actual use conditions" for each of their customers. These actual use conditions may include the network as well as the clinical use cases or workflows used by clinicians. This information is critical because the likelihood of finding a potentially serious defect in a networked medical device is much higher if the device can be tested under actual use conditions, meaning that the devices are installed on the network and used in a manner defined by clinicians.

The IEC/CD2 80001 draft standard recommends that medical device manufacturers are responsible for providing sufficient technical information regarding the connection of their devices to healthcare networks so that it may be possible to manage the risks related to having those devices connected to the network.

Examples of specific information device manufacturers should provide for a medical device whose intended use includes connection to a network is shown in Table 3.

The intended use of the medical device as it relates to the connection to the healthcare network.
Required network characteristics, configuration, and constraints of the healthcare network that are essential for the proper operation of the medical device.
Specific technical details describing the nature of the network connection and the flow of information between the medical device and the healthcare network.

Table 3. Information device manufacturers should provide for a medical device whose intended use includes connection to a network (*based on information contained in the 80001 draft*).

For their part, suppliers of healthcare networks also have a responsibility to provide information. Examples of the kinds of information they should provide are shown in Table 4.

Network specifications and technical manuals;
Recommended network configurations;
Relevant product upgrades and improvements;
Network security information;
Test strategies and acceptance criteria; and
Risk information

Table 4. Information that should be provided by healthcare network suppliers (based on information contained in the draft of 80001).

By collaborating with the healthcare organization's CE-IT staff and clinicians, device manufacturers and IT network equipment suppliers can share what they know and what they have done. The CE-IT staff can share details of their network, and clinicians can describe the "actual use environment." A discussion can ensue about where there may be potential issues. The group can then suggest ways to best address those issues by leveraging work already performed and documented by the device manufacturer.

If necessary, this information sharing can be accomplished under a mutual nondisclosure agreement so as to maintain confidential and/or proprietary information, as well as maintain critical network configuration information.

Device manufacturers need detailed information regarding the healthcare organization's network to do a more effective job of design validation and risk management. Table 5 shows information that must be provided so that appropriate validation and risk management activities can be planned and executed.

Network configuration parameters
Other devices (both medical and nonmedical) connected to the network that could possibly impact the medical device and vice versa
Software applications (both medical and nonmedical) running on the network that could possibly impact the medical device and vice versa
Policies related to installation of new devices (both medical and nonmedical) and software
Policies related to firewalls and anti-virus protection
Network security and change management policies

Table 5. Specific network information to help design validation and risk management activities.

In addition, clinical use cases and workflows that include the medical device need to be provided by clinicians so that design validation and risk management activities can be as effective as possible.

CE-IT staff and clinicians need to be actively involved in performing this design validation and risk assessment. To do this, some level of technical information regarding the functionality of the software embedded within the medical device, validation testing performed, risks identified and mitigated, etc., must be shared by medical device manufacturers.

CE-IT staff need to have specific training in design

validation and risk management practices and techniques, especially as they relate to networked medical devices.

Define Roles and Responsibilities

Clearly defining roles and responsibilities for risk management between the healthcare organization and device manufacturers is critical. Medical device manufacturers are already required to define responsibilities within their organizations for activities such as design validation, software validation, and risk management. This issue is addressed in the IEC/CD2 80001 draft.

Healthcare organizations need to take responsibility for the network they choose to install in their facility. This responsibility needs to extend far beyond that of ensuring that the network is functioning. It must include responsibility for managing risks associated with connecting devices from many manufacturers (medical and nonmedical) in order to ensure that each medical device connected to the network will operate in a safe and effective manner. This responsibility may require expertise in several technical disciplines, such as network management, security, clinical aspects of medical device operation and use, and risk management *(information from the 80001 draft)*.

The IEC/CD2 80001 draft defines the role of the IT risk manager. While this is a good start, the draft standard doesn't go far enough. What is needed is the impetus for device manufacturers, IT network suppliers, CE-IT staff, the IT integration risk manager, clinicians, and regulators to collaborate and to share information that can be used to reduce risk. For example, the IT integration risk manager should be responsible for documented compliance tests that can be used to ensure that the network is in compliance and remains in compliance as the network evolves over time.

Clinical Use Cases

Clinical use cases or workflows are essential for improving safety. Clinicians need to be actively involved in developing and documenting these use cases and, once documented, use cases need to be provided to medical device manufacturers so that this information can be reflected in the design, development, and validation of new or updated medical devices.

Figure 1 illustrates a clinical use case developed by blood banking technicians for a portion of what they do in a blood bank. Not only does this clinical use case illustrate ways in which a networked medical device may be used; it also provides for the establishment of common language between all of the stakeholders.

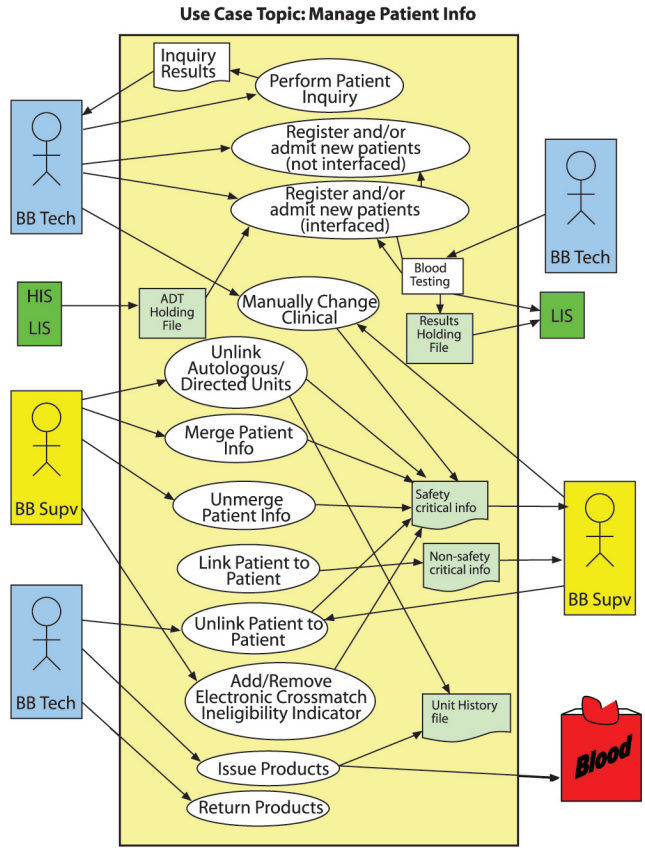

Figure 1. Example of a clinical use case for a blood bank. The information in the center box comprises the blood banking application.

Safety Cases

Other industries that rely on safety-critical systems have used safety cases to help provide visible evidence that a system is safe. A safety case provides documented evidence that supports a claim, such as the example shown in Table 6.

Supplier Audits

Supplier audits are a commonly used technique to assess a potential supplier's Quality System before making critical purchasing decisions. Healthcare organizations can perform supplier audits before making decisions to purchase IT network equipment as well as medical devices. During a supplier audit, the IT integration risk manager should be able to ask questions that would bear on the ability to integrate medical devices into the healthcare organization's network. This type of audit can also be used to determine whether potential IT network

Claim:	A specific medical device is safe to use when connected to a specific healthcare organization's network.
Arguments:	1. The medical device meets the following regulatory requirements [enumerate them] and complies with the following international standards [enumerate them].
	2. Safety requirements for the healthcare organization's network have been documented and provided to the medical device manufacturer.
	3. Clinical use case and workflow requirements have been documented by the healthcare organization and provided to the medical device manufacturer.
	4. The device manufacturer considered the specific healthcare organization's clinical use cases and workflow requirements in performing its risk assessment, design validation, and software validation.
	5. The medical device manufacturer has completed its risk management report and the results are within acceptable risk ranges.
	6. The medical device manufacturer has performed design validation and software validation testing, part of which included testing the device while connected to the specific healthcare organization's network.
	7. The healthcare organization's IT integration risk manager has received information from the IT network supplier indicating the network is functioning as intended.
	8. The IT integration risk manager has documented change control procedures in place that pertain to the healthcare organization's network, the devices (both medical and nonmedical) connected to it, the software installed on the network servers, and the overall configuration and security of the network. These procedures may require review of potential risks and revalidation of medical devices based on the nature of changes made to the network.
Evidence:	1. A risk management report specific to the medical device and the healthcare organization's network and clinical use case and workflow requirements has been reviewed and approved by the device manufacturer and the healthcare organization's IT integration risk manager.
	2. A design validation report specific to the medical device, the healthcare organization's network and clinical use case, and workflow requirements has been reviewed and approved by the device manufacturer and the healthcare organization's IT integration risk manager.

Table 6. Example of a Safety Case for a Networked Medical Device.

suppliers and medical device manufacturers are willing to work collaboratively with the CE-IT staff to provide the necessary supporting documentation for the safety case, and can help address safety issues down the road.

Conclusion

If we are to achieve the goal of improved safety and efficiency through the use of healthcare networks, all of the stakeholders have an obligation to create a common language and then collaborate and share information to an extent that goes well beyond that which happens today. For example:

- Device manufacturers need to share more information about design validation and risk as well as newly discovered discrepancies and how they might impact safety.
- IT network suppliers need to recognize that once their products are used in a healthcare environment, they share some responsibility to ensure that their products can continuously support this use.
- CE-IT staffs need to share the specific knowledge they each have about the network and how medical devices are used and how changes to their network may impact devices connected to the network.
- Clinicians need to provide clinical use cases based on the standard of care that involve networked medical devices.
- Regulators need to monitor safety and risk and provide appropriate guidance when needed to reduce risk.

Automating healthcare has long been viewed as a way to reduce both costs and costly mistakes. As healthcare organizations adopt new technologies, tradeoffs are made, and, in the end, we exchange one set of problems and risks for another set of problems and risks. The set of problems and risks that are incurred when medical devices are networked can be managed, but only if all of the stakeholders adopt a collaborative model where critical information is identified and shared. In order for networked medical devices to be as safe as "reasonably practical," medical device manufacturers, CE-IT personnel, and clinicians are going to need to develop a common language so that they can collaborate and share

relevant information and experiences. Emerging standards are starting to recognize that such collaboration is essential for improving the safety of networked medical devices.

References

1. The Joint Commission, Safely implementing health information and converging technologies, *Sentinel Event Alert*, Issue 42, December 11, 2008.
2. Stead W, Lin H, eds., *Computational Technology for Effective Health Care: Immediate Steps and Strategic Directions*, Committee on Engaging the Computer Science Research Community in Healthcare Informatics; National Research Council, 2009.
3. Eagles S. An introduction to IEC/CD2 80001: Aiming for patient safety in the networked healthcare environment, *IT Horizons*, 2008, 15–19.
4. FDA Quality System Regulation 21 CFR Part 820, October 7, 1996.
5. General Principles of Software Validation—Final Guidance for Industry and FDA Staff, January 11 2002.
6. ANSI/AAMI/ISO 14971:2007—*Medical devices—Application of risk management to medical devices*.
7. Draft Standard IEC/CD2 80001—*Application of risk management for IT-networks incorporating medical devices*, Committee Draft 2, Nov. 21 2008.
8. Draft Standard IEC/CD2 80001—*Application of risk management for IT-networks incorporating medical devices*, Committee Draft 2, Nov. 21 2008.

Additional Resources

1. Schrenker R. Sufficient evidence: Making the case for safety, *Biomed Instrumen Technol* 42(6); Nov/Dec 2008: 471–473.
2. Rakitin S. Coping with defective software in medical devices, *IEEE Computer*, April 2006: 40–45.
3. Jones PL et al., Risk Management in the design of medical device software systems, *Biomed Instrumen Technol* 36(4); Jul/Aug 2002: 237—266.
4. MD PnP Program http://mdpnp.org/Home_Page.php.
5. Jackson D, Thomas M, Millett LI, eds. *Software for Dependable Systems: Sufficient Evidence?* National Academies Press, 2007.
6. Bishop P, Bloomfield RA. Methodology for Safety Case Development. Safety-critical Systems Symposium, February 1998.
7. Institute of Medicine. *To Err is Human: Building a Safer Health System*. Washington, DC: National Academy Press, 1999.
8. —. *Crossing the Quality Chasm: A New Health System for the 21st Century*. Washington, DC: National Academy Press, 2001.

Steven R. Rakitin is a medical device software consultant currently serving on the AAMI/ACCE/HIMSS CE-IT Collaboration Working Group. He has written several papers on software quality and software-based medical devices and a book, *Software Verification & Validation for Practitioners and Managers*. He has presented invited papers, workshops, and tutorials at conferences worldwide for AAMI, ASQ, ASQ Biomedical Division, the HIMA, and IEEE. He has been involved with software development and quality for more than 35 years and has spent 19 years working in the medical device industry. As president of Software Quality Consulting, Inc. (www.swqual.com), he helps medical device companies comply with FDA regulations and standards in an efficient and cost-effective manner. He can be reached at steve@swqual.com.