Healthcare technology today is considerably different than it was 20 to 40 years ago. Yet, much of what is done by healthcare technology managers in support of medical technology has not changed. The tools and procedures still used by most clinical engineering services have evolved little to address some of the unique challenges posed by new healthcare technologies that are at once more pervasive, more complex and more susceptible to failures that may have catastrophic consequences for patients and healthcare operations.

Just how has the healthcare technology landscape changed?

Exponential Growth
There is ample evidence of the exponential growth in healthcare technologies in recent years. One of the largest healthcare providers in the United States, Kaiser Permanente, claims that between 1997 and 2007, their spending on health technologies and related procedures increased 9.3 fold! There is also evidence that this growth trend will only continue rapidly upward in spite of today’s tough economic climate. In a recent survey conducted by Boston-based L.E.K. Consulting of 200 hospital executives, 60% of those surveyed told researchers that they expect to spend more on medical devices in 2011, up from only 38% who saw spending increases a year ago. These increases are driven by the industry’s recognition that healthcare technology plays a critical role in enabling the delivery of quality, safe and effective care. It was the Institute of Medicine’s seminal report of 2000, “To Err is Human,” that claimed what most of us have come to accept today, that “technology ... has to be recognized as a ‘member’ of the work team.” We have come to heavily depend on this “member” of the team and our ability to deliver care can be severely compromised when that team member is not ready and available.

Increased Diversity, Complexity, and Connectivity
From advances in computerization, networking (wired & wireless), imaging, robotics, micro/nano technologies, genomics and telemedicine, healthcare technologies have significantly evolved in complexity and diversity and will only continue to do so at ever increasing rates. A 2009 Networking and Information Technology Research and Development (NITRD) Program report describes how “older generations of mechanical, analog and electromechanical devices ...
have been largely replaced by devices and systems based on information technologies” and how these devices/systems are “often connected to other devices in increasingly complex configurations, potentially creating systems of systems that span scales from tiny ... to ultralarge.” Formerly passive technologies have largely been replaced by new systems of systems (SoS) that actively control critical physiological processes and functions. A 2010 survey conducted by the College of Healthcare Information Management Executives (CHIME) concluded that 23% of medical devices in their inventory were networked; an additional 8% were network-capable but not yet connected.

Risk Management And the 80001 Standards

Changes associated with major increases in technology proliferation, diversity, complexity, and connectivity represent a major challenge and require a new mindset by those who are responsible for supporting these technologies. Perhaps foremost among the requisite mindset and skills necessary to address these new challenges is our adoption of and our approach to risk management. There is little evidence to indicate risk management is currently applied in little more than a narrow or superficial manner. Effective risk management is key to identifying substantive risks and applying available resources in a manner that most effectively addresses those risks. Absent effective risk management, resources are not applied where they are most needed and new vulnerabilities introduced by new technologies go unaddressed, often with dire consequences.

Our limitations in successfully managing the support of these new technologies is evidenced by that fact that, since the year 2000, there have been a growing number of reports by individuals and organizations of major medical system failures. Around 2004, Brian Fitzgerald of the U.S. Food and Drug Administration (FDA) had begun taking note of these reports. In December of 2005, he convened a meeting at FDA headquarters with experts from medical device manufacturers, healthcare providers (clinical engineering), and other relevant parties to discuss how to deal with the increasing number of complex systems and the new vulnerabilities they introduced.

That meeting concluded that while manufacturers had guidelines for effectively addressing risks associated with the development and manufacture of medical devices/systems (e.g., ISO/IEC 14971), there were no comparable, adequate guidelines that healthcare providers could employ to ensure the medical devices/systems they deployed were being appropriately

Update on 80001 Technical Reports

Four technical reports (TRs) have been completed to date and are currently going through the review and approval process:

- IEC TR 80001-2-1 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
- IEC TR 80001-2-2 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 TR 80001-2-4 Application of risk management for IT-networks incorporating medical devices – Part 2-4: General implementation guidance for healthcare delivery organizations

In addition, there are several TRs in preliminary stages of work. Titles are not firm yet, but the topics are:

- Guidance for responsibility agreements
- Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1
- Technical report on integration of alarm systems in the healthcare environment
supported. The outcome of the meeting was the establishment of a new workgroup under the auspices of the ISO/IEC. This workgroup was to include representatives from the world community of medical device manufacturers, healthcare providers, and standards development organizations who would develop guidelines for healthcare providers on how to best manage risks associated with the rapidly growing number of critical systems they were deploying.

U.S. and international experts (including medical device manufacturers, government and regulatory authorities, and clinical and information technology specialists from the healthcare provider community) met regularly over the next four years to develop a practical, high-level guideline that could be adopted by healthcare delivery organizations (HDOs) and that would be scalable to any size organization. In the summer of 2010, the final draft of ANSI/AAMI/IEC 80001-1:2010 Application of risk management to information technology (IT) networks incorporating medical devices was formally approved and the final document was released in October 2010 as an international standard.

The lack of updated tools and procedures—and an appropriate organizational framework in which to apply them—has been a major limiting factor in healthcare technology managers’ ability to effectively address the reality of today’s healthcare technology. With the adoption of 80001, these managers now have an important guideline from which to begin building those tools and procedures. These managers will also find that 80001 integrates well with one of the few other tools developed in recent years to address medical device security issues—namely, the Manufacturer’s Disclosure Statement for Medical Device Security (generally referred to as the MDS2). The MDS2 (which is currently being updated to more closely link to 80001) is a NEMA standard intended to provide medical device manufacturers with a standard means and format for communicating information about a medical device’s security features with healthcare providers in order for those providers to effectively manage security related risks associated with that device. The original MDS2 gained broad acceptance from both manufacturers and providers and it is likely the new version tailored to address 80001’s security elements will also.

Practical Advice on Implementing 80001

The three articles that follow describe the work of several technical committees that were involved in the development of 80001 under IEC Subcommittee 62A Joint Working Group 7. These articles describe the first set of guidance documents or technical reports (TR) under development and soon to be released. These documents are intended to provide additional assistance to organizations attempting to do an effective implementation of 80001:

- Nick Mankovich and Brian Fitzgerald’s article “Managing Security Risks with 80001” addresses issues associated with data security in networked medical devices and the kinds of processes appropriate for ensuring the integrity, availability and confidentiality of that device data. Ensuring data security will be critical and a substantial element in the future of all effective healthcare technology management services.
- Mike Papa’s article “Responsibility Agreements Ensure Accountability Under 80001” explains the rationale and key steps in implementing responsibility agreements. Responsibility agreements ensure the systematic identification of all stakeholders and the clear delineation of all responsibilities—a key aspect of any successful risk mitigation.
- Karen Delvecchio’s article “Step-by-Step Risk Management for Medical IT Networks” details how one technical report will provide HDOs with fundamentals of the risk management process and an overview of how these fundamentals should be applied. This article, and the technical report of which it is the subject, are particularly important because they describe processes which are critical to managing new complex technologies but with which most HDOs previously have had little exposure.

With the adoption of 80001, these managers now have an important guideline from which to begin building those tools and procedures.

To Get Involved

To get involved in the work of the committee developing the 80001 documents, contact Sherman Eagles at Sherman@80001Experts.com or Todd Cooper at Todd@80001Experts.com.
best to implement various aspects of the standard. There are likely to be some changes prior to final release of the Technical Reports and additional interpretations.

**Conclusion**

80001 and the technical reports described in the articles in this section represent a new approach specifically designed to prepare healthcare technology managers, clinical systems engineers and other stakeholders to effectively support today’s increasingly critical and complex technologies. Their help comes none too soon and will be instrumental in preparing us for the challenge.

**References**


