Standards for Safety, Security, and Interoperability of Medical Devices in an Integrated Health Information Environment

By Patricia A.H. Williams, PhD, MSs, BSc

Information sharing between healthcare organizations increasingly includes the use of electronic health records (EHRs) as well as data from medical devices that have been integrated into existing networks. When exchanging such data, providers should be mindful not only of the interoperability, privacy, and security of these devices, but also of their impact on patient safety. The protections required for safety, security, and privacy of health information across various information systems and medical devices are becoming increasingly complex.

Since medical devices are connected to hospital wireless networks, they are often vulnerable to hacking attempts.[1] The US Food and Drug Administration (FDA) recognized the problem in the Food and Drug Administration Safety and Innovation Act (FDASIA) report in 2014, proposing a "strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health information technology, including mobile medical applications, that promotes innovation, protects patient safety, and avoids regulatory duplication."[2]

Medical devices that include embedded software, stand-alone medical/health software, and "software as a medical device" (SaMD) are examples of the cutting-edge applications that are being used inside and outside a controlled hospital information sharing environment.

Fundamental privacy and security are a challenge for many healthcare organizations that may need assistance to address the potential vulnerabilities, particularly where networks include medical devices.[3] The increase in vulnerability arises from the nature of computer networks that demand plug-in methods of construction together with interconnectivity and seamless integration of multiple information systems involved in patient care.

In addition, the demand to improve the patient's hospital experience and the deployment of various information systems to support clinical and administrative needs, including medical devices on the network, further compound the potential privacy, security, and safety challenges.

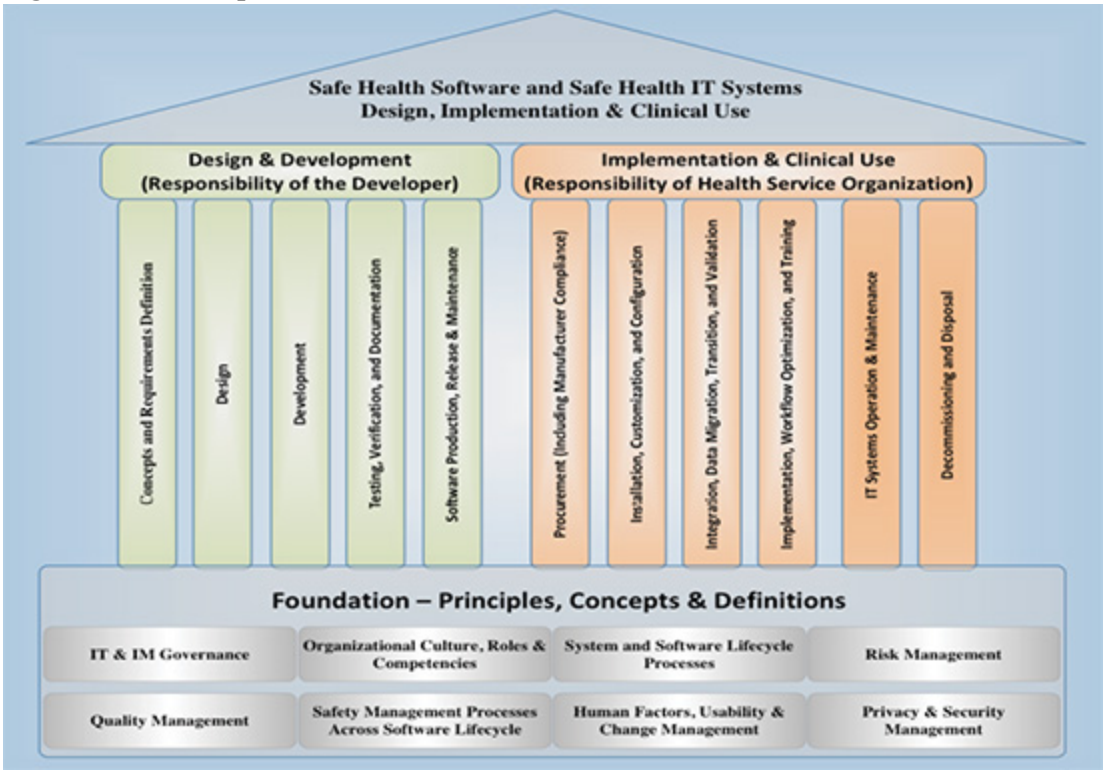
The Internet of Things (IoT) also contributes to a blurring of lines between information sources, devices, networks, and information technology applications. It will become more difficult to discern what is inside and what is outside of a network.[4]

Network construction and maintenance needs the help of skilled IT and—more importantly—skilled security personnel. Incidents where security and privacy compromise occurs, such as service attacks that block information input to a device or where the device battery is unnecessarily depleted, are major areas of concern.

Studies show that implantable devices, such as an implantable cardioverter defibrillator (ICD), are potentially susceptible to malicious attacks that violate the privacy of patient information and medical telemetry—and may experience malicious alteration to the integrity of information, including patient data in therapy settings.

One of the greatest challenges today—and arguably in the future—is how security and privacy in the context of safety-critical systems, such as implanted medical devices, will be addressed. For example, traditional approaches for security and access control may not always be suitable for implantable devices due to tensions between security (i.e., access for pre-authorized parties only) and safety (i.e., access for previously unauthorized parties in emergency circumstances). The goals between security, privacy, safety, and utility of devices in situ (in their natural position) may be at odds with one another.[5]

Figure 1: The Scope of IEC/ISO 80001 Standards Series



Standards to Address Safety, Security, and Privacy of Medical Device Information

The key to enabling patient safety is standardization.[6] The new standard published by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), IEC 82304-1:2016 Health Software–Part 1: General requirements for product safety, is focused on patient safety of health software. This standard emphasizes that software development has been identified as a major area that can compromise patient safety.

The Joint Working Group 7 (JWG7) of the ISO Technical Committee 215 (ISO/TC215) Health Informatics, which developed the new standard, includes software developers, medical device manufacturers, patient safety experts, and security, privacy, and risk management experts. Guidance from collated worldwide expertise can contribute to operational aspects of information security, privacy, and safety as well as underpinning the information and security governance that organizations should demonstrate. It is with the increasing challenges of privacy and security in healthcare that ISO/TC215 JWG7, in collaboration with the IEC Sub-Committee 62A: Common aspects of electrical equipment used in medical practice, are conducting a systematic review of the series of standards entitled IEC/ISO 80001 Application of risk management for IT networks incorporating medical devices. The standard was originally published in 2010.

The revision to the IEC/ISO 80001 standard series addresses the breadth of the use of medical devices from inception, development, deployment, and continued use to retirement, with the points of transition between manufacturers, implementers, and users identified as a key area for improvement (see Figure 1 above).

A fundamental part of the IEC/ISO 80001 standard series is taking a broader perspective on the development and use of medical devices, and encapsulating the foundational principles, concepts, and definitions that would apply across the entire device and information lifecycles. The standard covers the following areas:

- Governance in Information Security (IS) and Information Management (IM)
- Organizational culture, roles, and competencies
- Systems and software lifecycle processes
- Risk management
- Quality management

- Safety management processes across software lifecycle
- Human factors, useability, and change management
- Privacy and security management

The focus on these areas aims to provide comprehensive articulation and consistency across the device and information lifecycles. Commonly, these areas have not been addressed in a consistent way. They may have differing importance depending on the stakeholder involved, and differing requirements depending on the context of use and their place along the device and information lifecycles.

In healthcare, the context of information use is vitally important, and includes people, processes, and associated technology, including medical devices, together with an understanding of data flow, workflow, and intended use. The stakeholders along the lifecycle need to understand how the areas listed above affect how the medical device is expected to function, as well as how it may fail, and the consequent impact of such failure.

A particularly important task is to identify and manage the potentially risky points of transition, including the transition from device design/production (responsibility of the manufacturer) and implementation/use (responsibility of the healthcare organization). A separate component of the ISO/IEC 81001 standards series will address the necessary comprehensive guidance to ensure a consistent approach to patient safety in the design and use of medical devices.

Ultimately, the systematic review of this important family of standards (ISO/IEC 80001) is aimed to establish guidance and controls applicable to a technical landscape that encompasses future systems and architectures such as Bring Your Own Device (BYOD), the Internet of Everything (IoE), Services Oriented Architectures (SOA), and "Anything as a Service" (XaaS). The guidance has to consider the increasing socio-technical and adaptive systems environment, and be applicable to all healthcare organizations regardless of size. ?Importantly, all guidance will need to be scalable to all manufacturers and software developers—large and small. These objectives are a significant challenge and will require risk management that is sufficiently broad to address such a multifaceted landscape.

If you are interested in participating in the development of the ISO/IEC standards, please contact Diana Warner, director of standards at AHIMA and Secretary of ISO/TC215 at diana.warner@ahima.org.

Notes

[1] Williams, Patricia A. H. and Andrew J. Woodward. "Cybersecurity Vulnerabilities in Medical Devices: A complex environment and multifaceted problem." *Medical Devices: Evidence and Research* 8 (2015): 305-316.

[2] US Food and Drug Administration. "FDASIA Health IT Report. Proposed Strategy and Recommendations for a Risk-Based Framework." April 2014.

[3] Rushanan, Michael et al. "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks." Proceedings of the IEEE Symposium on Security and Privacy, May 18-21, 2014, San Jose, CA.

[4] Williams, Patricia A. H. and Vincent McCauley. "Always Connected: The Security Challenges of the Healthcare Internet of Things." Presentation at the IEEE World Forum on Internet of Things, December 12-14, 2016, Reston, VA.

[5] Rushanan, Michael et al. "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks."

[6] Glickman, Michael and Anna Orlova. "Building Interoperability Standards and Ensuring Patient Safety." *Journal of AHIMA* 86, no. 11 (November-December 2015): 48-51.

Patricia A. H. Williams (patricia.williams@flinders.edu.au) is the CISCO chair and a professor of digital health systems at the School of Computer Science, Engineering and Mathematics at Flinders University.

Article citation:
Williams, Patricia A.H. "Standards for Safety, Security, and Interoperability of Medical Devices

in an Integrated Health Information Environment" *Journal of AHIMA* 88, no.4 (April 2017): 32-34.