Building Interoperability Standards and Ensuring Patient Safety

Save to myBoK

By Michael Glickman, MSE, and Anna Orlova, PhD

Anyone who has ever developed a standard knows well the many challenges that must be surmounted. Once a standard is published, however, it's not the end but in many respects only the beginning. Moving standards from specification to practice requires an equivalent if not greater effort, as does ensuring that standards are not stuck at a point in time but are "living" and are periodically updated to reflect experience from users as well as advances in the state-of-the-art health information and communication technology. More importantly, individual standards have to work together to enable information sharing and interoperability across various health information and communication technology (HICT) products.

The result of 16 years of standards development has led the International Organization of Standardization (ISO) Technical Committee 215, Health Informatics (ISO/TC 215) to the practical realization that a "bundle" of individual standards is required to create interoperable health information technology (health IT) standards that will ensure both adoption and sustainability.

Building Interoperability Standards

A bundle of individual standards that work together to enable interoperability represents a high-level standard specification—an assembly of individual standards that move information from sender to receiver. Interoperability standards are harmonized and intergrated individual standards constrained to meet healthcare and business needs for sharing information among organizations and systems for a specific scenario (use case) of health information exchanges.

According to the Health Level Seven (HL7) definition, interoperability is comprised of the following three components (pillars):

1. Semantic interoperability—shared content
2. Technical interoperability—shared information exchange infrastructure (transport)
3. Functional interoperability—shared rules of information exchanges (i.e., business rules and information governance (IG), "the rules of the road")

Thus, the interoperability standard—a bundle or assembly of individual standards—has to include individual standards from these three components of interoperability. The concept of "a bundle" of individual standards working together was first introduced by the Health Information Technology Standards Panel (HITSP, www.hitsp.org) in 2005. HITSP operated as a public and private collaborative supported through a contract from the Office of the National Coordinator for Health IT (ONC) to the American National Standards Institute (ANSI). The HITSP bundle was formally called "Interoperability Specification (IS)." Between 2005 and 2009, HITSP developed 19 ISs for various national use cases including Electronic Health Record (EHR) Laboratory Result Reporting (IS 01), Biosurveillance (IS 02), Consumer Empowerment (IS 03), Quality (IS 06), and Consultation and Transfer of Care (IS 09), among many others.

HITSP IS included specific individual standards grouped by the following categories:

- **Semantic Interoperability**
    - Data Standards (vocabularies and terminology standards)
    - Information Standards (reference information models, information templates, and other)
- **Technical Interoperability**
    - Information Exchange Standards (message-based and document-based)
    - Identifier Standards

  - Privacy and Security Standards
- **Functional Interoperability**
  - Functional Standards (requirements for health information and communication technology derived from the analysis of the use case)
  - Business Processes Standards (guidelines and best practices described in the use cases)

<

Figure 1: Number of Individual Standards Included in the HITSP Biosurveillance IS 02

Standard Category	**Number of Standards**
Semantic Interoperability (Content)	
Data Standards	28
Information Standards	17
Technical Interoperability (Transport)	
Information Exchange Standards	46
Identifier Standards	11
Privacy and Security Standards	5
Functional Interoperability (Rules)	
Functional Standard	1
Business Processes Standards (guidelines, best practices, use cases)	1
Total	**109**

For example, HITSP Biosurveillance IS 02 included 110 individual standards (see Figure 1).[1] This assembly of standards supported a charge formulated in the National Biosurveillance Use Case of transmiting “essential data from electronically enabled healthcare to authorized public health agencies in real-time.”

Essential data included 40 data elements defined by the Centers for Disease Control and Prevention (CDC). Biosurveillance use case was the first of the three national use cases developed for HITSP by the American Health Information Community (AHIC)—an ONC advisory committee that identified priorities for health IT interoperability and developed national use cases. The first three use cases included biosurveillance, EHR laboratory result reporting, and consumer empowerment. A total of 152 national use cases were developed by AHIC between 2005 and 2009. These use cases served as business requirements for the HITSP interoperability specifications.

Built upon the HITSP methodology, ISO/TC 215 decided to move forward with developing interoperability standards. The working title for the ISO "bundle" is "Standards Reference Portfolio (RSP)." The first domain selected for developing ISO RSP is clinical imaging. The work has been conducted in collaboration between ISO/TC 215 and DICOM, a standards development organization.[2]

ISO RSP includes standards for content and payload (semantic interoperability), transport (technical interoperability), and rules (functional interoperability) (i.e., standards for information governance and information management practices—which are strategic AHIMA imperatives).[3,4,5,6]

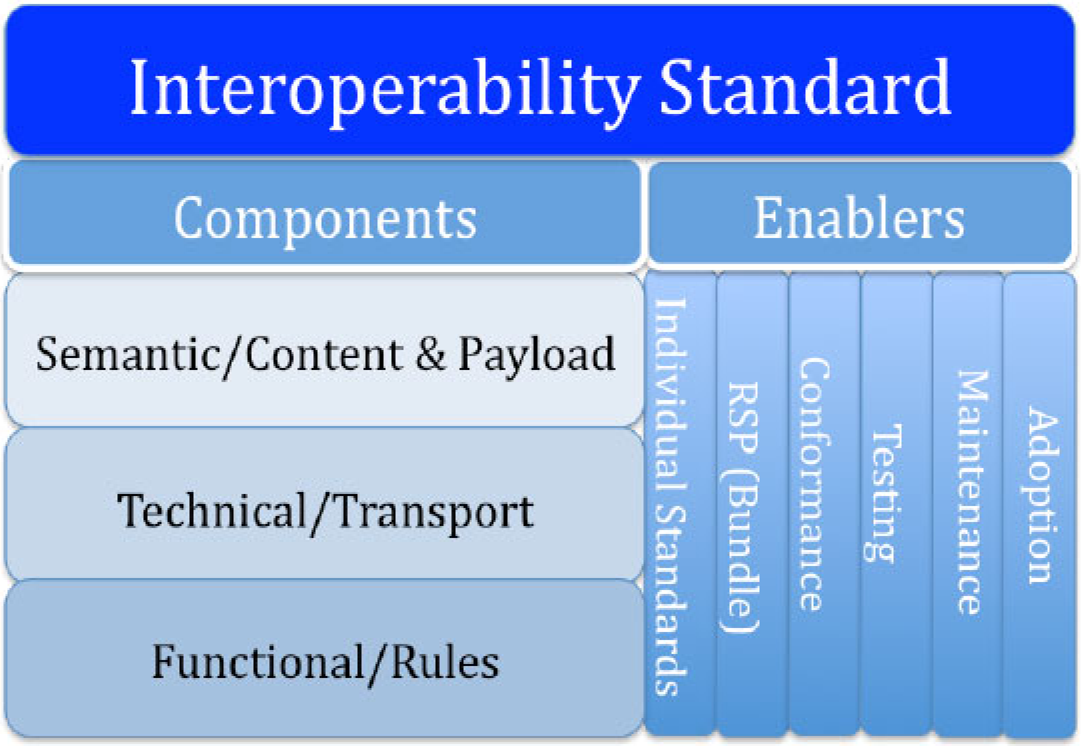
Critical constituents of the RSP bundle's functional interoperability standards include standards that enable data capture (information availability), data quality validation (data integrity), data protection (capture of patient consent for healthcare procedure as well as information sharing; protection of privacy, confidentiality, and security of information), and other standards for information governance principles in healthcare defined by AHIMA.[7]

ISO RSP also defines conformance criteria, which are statements that specify how various individual standards should work together. These criteria will be used by vendors to test RSP and to deploy standards into their products. They also will be used in HICT certification processes, so users know that the product is compliant with the interoperability standard.

Maintenance is important to keep RSP up-to-date. In order to ensure that standards remain relevant ISO has developed directives that govern all ISO standards. One of these is the compulsory five-year systematic review when standards developers employ a systematic review process to determine whether a standard is (a) still relevant and in use, (b) is no longer needed and should be retired, or (c) is in use but should be revised to ensure its continued value to the industry. Adoption and continuing feedback from the users regarding the standards-based capabilities allows them to keep the standard updated to meet user needs.

Figure 2 below presents the interoperability standard framework with various RSP components and enablers.

Figure 2: Interoperability Standard Framework: Components and Enablers



Ensuring Patient Safety through Interoperability Standards

One of the keys of health IT adoption is enabling patient safety while using the means of standards-based health information and communication technology. Specific aspects of ensuring health technology safety through standardization is specified in the ISO/IEC 80001 standard published in 2010.[8] It was up for a systematic review in 2015. This standard was born out of the recognition that networked medical devices are increasingly being deployed on general purpose IT infrastructure. Though the manufacturers have to rigorously apply risk management to identify and manage potential safety issues and receive regulatory clearance to place their technology on the market, once the product is purchased, implemented, and placed in use, risk management processes are rarely applied to the resulting network of integrated devices, health information and communication technology systems, and applications. Unintended consequences that compromise patient safety had been occurring far too frequently and overall confidence in the technology had been suffering accordingly.

Specific safety risks associated with non-interoperability of health IT products include:

- Data quality, misidentification and integration of patient data from multiple sources (record matching on a patient represents a critical record management step, so that the information from one patient cannot be added to the chart of another patient)
- Data accuracy, availability, and integrity issues due to configuration, security, or IT operations failures
- Decision support failures due to incorrect or outdated medical logic, reference data, algorithms or alert triggers
- Failures and inconsistencies in delivery, integration, or presentation of diagnostic information results
- Failures and inconsistencies in delivery, integration or presentation of therapy information (such as radiotherapy information)
- Insufficient attention to workflow, human factors, change management, or training of clinicians
- Privacy breaches, data governance issues, or other causes that erode provider and consumer confidence

The risk management for health information and communication technology can be formulated in four questions:

1. What can go wrong?
2. How can it happen?
3. What can be done about it?
4. How do we know we have done enough?

The ISO/IEC 80001 standard evaluated under the ISO systematic review process demonstrated that:

- Yes, the ISO/IEC 80001 standard remains highly relevant, even more so given the increasingly complex health IT environments and the increased integration of medical devices and various health IT products
- No, ISO/IEC 80001 standard has not been widely implemented; as much as ever, it is widely recognized as a key component of addressing safety and security when interoperable technology is deployed
- Yes, the state-of-the-art health information and communication technology has been advanced
- Yes, much has been learned about what is needed to ensure the safe use of information in healthcare

There is a need for new understanding of medical device safety, and of the safety of any collection of objects running software and being connected, such as the Internet of Things, in the context of a specific use or use case.

ISO/TC 215 Health Software Ad Hoc Group looked at the broader issue of health software safety standards to admit that "while our initial focus was on health software, we have recognized that the architecture of health software safety standards must also address the safety of the broader health IT system, and the socio-technical environment of which health software is a component."

This "environment" includes not only the information technology (i.e., hardware, software, networks, interfaces to other systems and data), but also the:

- People (i.e., clinicians, patients, consumers, caregivers, administrators)
- Care processes (i.e., clinical workflow, decision algorithms and care protocols)
- Organization (i.e., capacity, governance, configuration decisions about how health IT is applied)
- External environment (i.e., regulations, public opinion, ambient conditions)

The group further focused on defining end-to-end safety management strategy, leveraging standards in areas such as risk, quality, security, IT lifecycle, information governance, etc., and identifying gaps that need to be filled. The report finalized during spring 2015 identified the technology lifecycle over which safety must be established and maintained. Eight key topics are integral to achieving health information and communication technology safety. Grouped under the three categories—people, technology, and policies—they include:

People

1. Organization's culture, roles, and competencies
2. Human factors, usability, and change management

Technology

3. Systems and software lifecycle processes
4. Safety management processes across software lifecycle

Policies

5. IT and information governance
6. Risk management
7. Quality management
8. Information privacy and security management

The ISO/IEC 80001 standard is an example of a standard that will be included in the ISO/TC 215 RSP (bundle) to ensure that standards included in the RSP properly address risks associated with semantic, technical, and functional components of interoperability.

Notes

1. Health Information Technology Standardization Panel (HITSP). "Biosurveillance Interoperability Specification (IS) Number 02." 2009.
2. Digital Imaging and Communication in Medicine (DICOM).
3. Tech Terms. "Payload definition."
4. Cohasset Associates and AHIMA. "A Call to Adopt Information Governance Practices: 2014 Information Governance in Healthcare." 2014.
5. Cohasset Associates and AHIMA. "Professional Readiness and Opportunity: 2015 Information Governance in Healthcare." 2015.
6. AHIMA. "A Call to Adopt Information Governance… ."
7. Ibid.
8. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). "ISO/IEC 80001-1:2010. Application of risk management for IT-networks incorporating medical devices—Part 1: Roles, responsibilities and activities." October 1, 2010.

Michael L. Glickman (MGlickman@CNAInc.com) is CEO of Computer Network Architects and chair of ISO/TC 215 Health Informatics. Anna Orlova (anna.orlova@ahima.org) is senior director for standards at AHIMA and an ISO/TC 215 member.

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