Overview of Health IT Standards

Save to myBoK

By Anna Orlova, PhD

Health IT Standardization is the process of agreeing on standards that allow electronic exchange of data, information, and knowledge between disparate data systems. The goals of standardization are to achieve comparability, compatibility, and interoperability between independent systems; to ensure compatibility of data for comparative statistical purposes; and to reduce duplication of effort and redundancies.

The Health Information Technology Standards Panel (HITSP), a public-private partnership led by the Office of the National Coordinator for Health IT (ONC) that operated from 2005 to 2010, developed a methodology for grouping health IT standards in a meta-standard, or interoperability specification, that defined the number of various standards that have to work together to collect/share/exchange data between systems for a specific purpose (use case). Thus, HITSP's Biosurveillance Interoperability Specification, which was charged to transmit essential data (a total of 40 data elements) from electronically enabled healthcare facilities to authorized public health agencies in real time, identified 107 standards that needed to work together (see Table 1 below).[1]

Table 1. Health IT Standards for Biosurveillance Use Case

Standards Categories	**Number of Standards**
Data Standards	28
Information Content Standards	17
Information Exchange Standards	46
Identifier Standards	11
Privacy and Security Standards	5
Functional Standards	0
Other Standards	0
Total	107

Today in the US, interoperability between health IT products, such as data sharing, has proven to be very difficult to establish. There is an urgent need to reconsider the current approach to health IT standardization and revisit the experience and lessons learned from other efforts, such as HITSP, to transition to a robust methodology for standardization of health IT products. More work is needed to specify standards that must work together to further interoperability.

An Overview of Standards Terms and Definitions

A standard is a definition, set of rules or guidelines, format, or document that establishes uniform specifications, criteria, methods, processes, or practices that have been approved by a recognized standard development organization (SDO), or have been accepted by the industry as "de jure" standards, such as formal legal requirements. There are also "de facto" standards, which have become standards because a large number of companies have agreed to use them.

To support the collection and use of data, information, and knowledge in healthcare, health IT standards are utilized in health IT products, such as electronic health record (EHR) systems, laboratory information management systems (LIMS), radiology and pharmacy information systems, public health and research information systems, and a growing number of mobile health IT applications.

HITSP has identified seven health IT standards categories, listed in Table 2 below with respective examples.

Table 2. Health IT Standards Categories

Standards Categories	**Examples**
Data Standards	Vocabularies and terminologies
Information Content Standards	Reference Information Models (RIM)
Information Exchange Standards	Message-based and structured document-based
Identifier Standards	National Provider Identifier (NPI), specimen identifier, etc.
Privacy and Security Standards	Access control, audit, electronic consent
Functional Standards	Work processes, workflow and dataflow models
Other Standards	• Business standards (i.e., clinical guidelines) • Information and Communication Technology (ICT) standards (i.e., Internet protocol, programming languages, etc.)

Source: Health Information Technology Standards Panel. www.hitsp.org.

Data Standards Defined

Data standards are documented agreements on representations, formats, and definitions of data. Data standards provide a method to codify information captured in the course of doing business in valid, meaningful, comprehensive, and actionable ways.

Data standards are represented in vocabulary and terminology standards, including:

- International Classification of Diseases (ICD)
- INTSDO/Systematic Nomenclature for Medicine (SNOMED)
- Logical Observation Identifiers Names and Codes (LOINC)
- Unified Code for Units of Measure (UCUM)
- Accredited Standards Committee X12 (HIPAA Transaction Format)
- Current Procedural Terminology (CPT)

Information Content Standards Defined

Information content standards define the content of information exchanges. First level information content standards define the structure and organization of the electronic information content. The Health Level Seven (HL7) Reference Information Model (RIM) is a pictorial representation of clinical content as discrete objects, or data elements, that can be generated, shared, and used in a lifecycle of healthcare events between participants. RIMs are models of information, or data objects, that are shared and reused between domains of care, such as clinical encounters, laboratory testing, prescriptions, billing, public health reporting, and research. As such, there are standards for data representation across these domains.

Second level information content standards define a "package" in which information and data objects are represented, such as in a string, in message-based standards (HL7 Versions 2.x and 3.0), or a structured document (form, record) in document-based standards (HL7 Clinical Document Architecture (CDA) for Continuity of Care Document (CCD)) and HL7 Fast Health Information Resource (FHIR). The CDA standard provides both a standardized header containing metadata about the document as well as a wide variety of clinical content organized into sections. The FHIR standard is based on the 80/20 rule, which dictates that data elements should only be added to the standard if 80 percent of the systems use them. FHIR allows for extensions of additional data elements in a manageable process.

Information Exchange Standards Defined

Information exchange standards offer a uniform way of sending, receiving, and exchanging information. There are two types of information exchange standards—message-based and document-based. Message-based information is sent as a string in a message, while document-based information is sent as a structured or unstructured document, such as an e-mail, form, record, or PDF. Message-based information exchange standards are point-to-point communication between health IT systems. HL7 Version 2.3 is the most commonly used message-based standard in health IT products in the US.

Table 3 below presents five ways to exchange health-related documents electronically using secure e-mail, web services, and health information exchanges (HIEs). It also shows the examples of document-based information exchange standards by option developed by Integrating the Healthcare Enterprise (IHE).[2]

Table 3. Document-Based Information Exchange Options and Standards

Document-Based Information Exchange Options	Standard Examples

1. Secure broadcast e-mail	Simple Mail Transfer Protocol (SMTP) is the Internet protocol used to transfer electronic mail between computers
2. Secure e-mail to a known recipient	SMTP and IHE Cross-Enterprise Document Media Interchange (XDM) Standard
3. Web services	IHE Cross-Enterprise Document Reliable Interchange (XDR) Standard
4. Information exchange within HIE	IHE Cross-Enterprise Document Sharing (XDS.b) Standard
5. Information exchange across HIE	Cross-Community Access (XCA) Standards

Message-based standards are used to support ongoing data sharing in a real time. They convey status information and updates related to the same dynamic object, such as laboratory orders. Documents are information "snapshots" at a particular time, so document-based standards are used to transmit "static" content usually when the process is done, including laboratory reports, encounter summaries, and public health reports. Both message-based and document-based approaches may coexist depending on the user needs. A use case can determine what paradigm represents the better solution for a user.

Identifier Standards Defined

Identifier standards provide a universal method to identify entities such as a patient, a provider, a healthcare organization, a payer, a vendor, or a product. Identifiers are the lexical tokens that name entities in all information systems, which is essential for any kind of symbolic processing.

A number of identifier standards have been adopted for healthcare in the US including a National Standard Identifier for Individuals and Organization Health Care Providers and a national employer identification number (EIN) adopted for use in all electronic administrative and financial transactions, including claims and claim payments. The creation of a national patient identifier standard is still not done, though many organizations have implemented internal master patient index (MPI) applications that have systematic matching and merging of records in information systems to create an accurate, unique health record for each individual. There are other identifiers for medicines, specimens, medical devices, and other entities.

Privacy and Security Standards Defined

Privacy and security standards serve to ensure information security and confidentiality. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Security refers to physical, technological, or administrative safeguards or tools used to protect identifiable health information from unwarranted access or disclosure. Security is the set of actions an organization takes to protect that information. Confidentiality has been defined by the International Organization for Standardization (ISO) as "ensuring that information is accessible only to those authorized to have access" and is one of the cornerstones of information security.

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Provisions introduced the first comprehensive federal privacy and security rules and guidelines for standardization of electronic data exchanges. In response to HIPAA, various standards were developed to enable transport security, identification of persons and systems, privilege management and access controls, audit, policy agreements, and pseudonymization. These standards are viewed as the information technology infrastructure (ITI) standards that must be supported by any system participating in electronic data exchanges. The IHE ITI Technical Framework is a conduit of infrastructure standards for systems interoperability and contains a number of standards for information security.

Functional Standards Defined

In healthcare, functional standards—or functional requirements—describe the people and information systems as well as the functions and features that are required in a software application. These standards are defined by a qualified group of domain experts and stakeholders. Functional requirements are derived from the description of a user's business activities to explain why a software application is needed and describe what the software application must do. Determining this is done by translating business requirements into the following five functions of the information system:

1. Collect/Input Data (i.e., get data into the software application)
2. Manage Data (i.e., verify, store, update, and dispose)
3. Analyze Data (i.e., group data by similar attributes, such as location, condition, etc.)
4. Integrate Data (i.e., send/receive data from various data systems/sources)
5. Generate Output (i.e., create reports, summaries, alerts, notifications, etc.)

A functional standard is a vehicle to ensure that the work processes of users related to a particular business activity, including activities such as patient care management or public health surveillance, that involves the use of electronic data exchanges are well understood and agreed upon first by users themselves and then communicated clearly to the developers as functional requirements for a software application.

Notes

[1] Health Information Technology Standards Panel. "Biosurveillance Interoperability Specification (IS-02)." www.hitsp.org/InteroperabilitySet_Details.aspx?MasterIS=true&InteroperabilityId=49&PrefixAlpha=1&APrefix=IS&PrefixNumeric=02.

[2] Witting, Karen and John Moehrke. "Health Information Exchange: Enabling Document Sharing Using IHE Profiles." Integrating the Healthcare Enterprise (IHE). January 24, 2012. www.ihe.net/Technical_Framework/upload/IHE_ITI_White-Paper_Enabling-doc-sharing-through-IHE-Profiles_Rev1-0_2012-01-24.pdf.

Anna Orlova (anna.orlova@ahima.org) is senior director of standards at AHIMA.

Article citation:
Orlova, Anna. "Overview of Health IT Standards" *Journal of AHIMA* 86, no.3 (March 2015): 38-40.