

Which “Standards” Are We Discussing?

Willa H. Drummond, MD, MS (Informatics)
Professor of Pediatrics and Physiology
Member, AAP Steering Committee of the Council on Clinical Information Technology

Division of Neonatology, Department of Pediatrics
Box 100296 JHMHC
University of Florida College of Medicine
Gainesville, FL 32610

DrWilla@icudatasystems.com

January 10, 2006

Introduction

Recent government mandates to improve clinical health care by using information technology stimulated broad interest in rapid adoption of computerized technologies. The envisioned end-to-end integrated clinical functionality requires health care computer systems to adhere to emerging “standards”. “Standards” can mean software formats for computer-to-computer communication, computerized semantic maps of medical terminology, organized health care data element templates, or generic management quality. Conceptual confusion and communication failures across the professions, often unrecognized, are nearly universal. Each of the professions uses “technical jargon” words that reference specific and unique concepts and mental models of reality. The word “standards” exists in each profession’s technical vocabulary. But the word “standards” means something very different to the different experts.

Unfortunately, nearly everybody involved in the computerization effort struggles with semantic confusion caused by the use of the word “standards” to convey many different meanings across the technical jargons and vocabularies of the involved professional disciplines. What are “standards”?

The Merriam-Webster Online Dictionary has many definitions for the word “standard”. Non-computer people generally think “standards” are, “**3** : *something established by authority, custom, or general consent as a model or example* : and; **4** : *something set up and established by authority as a rule for the measure of quantity, weight, extent, value, or quality.*” (). These definitions relate poorly to the technical meaning of “standards” in the minds of the electrical engineers, computer scientists, programmers, or to the many professional meanings understood by physicians, nurses, health administrators, government and funding bureaucrats, quality assurance specialists, and lawyers.

For example, when a physician and a computer scientist discuss healthcare “standards”, the physician often thinks of “standards” as a quality indicator, as in “standard of practice”, while the computer scientist knows “standards” as sets of nationally or internationally agreed-upon, precise software programming structures that enable two different computer systems to communicate with each other for data exchange. In a different scenario, the quality assurance officer of a large healthcare system might understand “standards” as either a quality of care indicator, or as a means for linking the enterprise’s different computer systems to the QA management database. The “QA” officer’s concepts of “standards” will depend on his specific training, and perhaps on whether the conversation involves a physician or a computer programmer. An electrical engineering contractor, discussing networking “standards” with a nurse-charting system’s implementation administrator, is probably referring to the IEEE “stack” of “protocols” that defines how electrons flow across wires and through switches, essentially organizing how “the web” works electronically (), while the nurse administrator may be thinking the conversation concerns HIPAA security issues. ()

The Situation

An “Information System” is some type of system that manages some form of information. “Clinical information systems” are information systems that provide access to, and methods for, recording and managing clinical data. Examples include paper and electronic flow sheets, physician and nurse daily notes, physician orders, prescriptions, radiology results, lab orders and results, history and physical reports, and admit and discharge summaries. Most computerized information systems in health care settings need to be linked for full clinical utility. Commercial and locally build order entry, note generating and imaging systems, local and national lab and pharmacy systems etc. must contribute clinical data of the clinic’s or hospital’s central information system (HIS) for

mandated archiving. Ensuring accurate communication between different types and ages of computer systems is difficult. Are “standard” codes used in one system the same as in another vendor’s system. Do the data have a “standard” structure? What “standards” are needed to integrate all the information? The success of healthcare data integration is ultimately based on the use of “standards”.

Intercommunication Standards & HIPAA (Haugh 2000)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (P.L. 104-191, Title II, Subtitle F) is a one of the largest pieces of health care legislation in history. President Clinton signed HIPAA into law on August 21, 1996. HIPAA, as passed, had three stated goals: 1) to improve access to health insurance; 2) to reduce fraud and abuse; and, 3) to increase the efficiency and effectiveness of the health care system. (Friedrich 2001)

The Administrative Simplifications section of HIPAA mandated use of open “computer communication standards” for accessing, transmitting and storing electronic medical data. These mandates were coupled with federal laws designed to ensure the privacy and security of personally identifiable patient information that was processed by computer (~ “security standards”).

The HIPAA legislation mandated that specific clinical vocabulary code sets and computer communication strategies (both called “standards”) be decided at a national level and implemented by specific dates, now all past. The technical work for completing health care “computer communication standards” is in progress now. No one “standard” was, or is, completely finished. Voluntary, underfunded, standards-setting groups meet regularly. New computerized clinical systems will be required to be “HIPAA Compliant”. All the aspects of HIPAA compliance rules are an enormous “work in progress” at the time of this writing (Winter 2005).

HIPAA Mandates: Codes and “Standards”

Before HIPAA, more than 400 different formats for electronic transactions had been created for computer communications between providers and health plans (DHHS, 2000). HIPAA reduced the number to two electronic transaction/computer communication standards for health care administrative and financial communications and eight clinical code sets. (DHHS, 2000) “Open Standards” in HIPAA means a “computer communication standard”. The HL7 (Health Level 7) and ASC_X12N computer communication standards provide uniform programming structures to organize different vendors’ clinical, lab, or hospital information systems software for meaningful medical and administrative information exchange. These “computer communication standards” are a software template that has a specific place assignment where programmers insert needed information, such as a patient identifier, whether they are writing a lab system, a clinical system, or an administrative system.

A “standard code set” is an organized, agreed-upon system of codes for listing data elements, such as tables of terms, medical diagnosis codes and medical procedure codes. “Standard” HIPAA-defined “Codes” are precisely formatted numbers and letters that match some clinical concept, such as a diagnosis, medication or treatment. (DHHS, 2002) Code sets now defined as standard (non-technical use of word) under the HIPAA legislation are:

- 1) ICD-9-CM (International Classification of Diseases, 9th or 10th Edition, Clinical Modification), used for diagnoses and hospital patient services codes.
- 2) HCPCS (Health Care Financing Administration Common Procedural Coding Systems), used for physician and institutional services to report supplies, devices, durable medical equipment and generic drugs under Medicare plans (DHHS, 2002).
- 3) CPT (Current Procedural Terminology) is used to code physician services.

- 4) CDT (Current Dental Terminology) is used to code dental services.
- 5) NDC (National Drug Code) is used only for medications and drug systems for retail pharmacies. (DHHS, 2002).

Computer communication “standards” defined under HIPAA are:

- 1) ASC_X12N, Version 4010 (Accredited Standards Committee, 2005) for health claims, attachments and encounters, payment and remittance advice, claim status, eligibility, referrals, health care enrollment, health plan premium payments and first report of injury.
- 2) HL7 (Health Level 7) is named for the level of the conceptual “IEEE Stack” where a software application’s structure is defined. The HL7 “standard” defines a specific computer reading structure (similar to a blank paper template) where programmers to insert a “coded” patient identifier, lab order, lab result, units of measure, local name of lab request and standard name of lab, etc. (HL7, 2005)

Problems quickly arose with attempts to apply administrative “code sets” (CPT and ICD 9) to clinical computerized medical records, because the approved administrative code sets are inadequate for full clinical documentation, especially in pediatrics and neonatology. According to Chute (2002), administrative classification systems such as ICD-9 and CPT lose more than half the underlying, detailed clinical information because the codes were developed for billing purposes, not for managing detailed clinical data in patient care venues.

HIPAA mandated clinical code sets (or “standard” vocabularies) either in use, or nearly ready for release are:

- 1) LOINC (Logical Identifier Names and Codes) is used for very precise laboratory and clinical messages, like “fasting whole blood glucose” or “sitting systolic blood pressure, upper extremity”. (LOINC ref)

- 2) SNOMED (Systematized Nomenclature of Medicine) is used for very specific diagnostic messaging, such as “ruptured appendix with peritonitis”. (SNOMED Ref)
- 3) NIC (Nursing Intervention Classification), NOC (Nursing Outcome Classification), and NANDA (North America Nursing Diagnosis Association) are used for nursing diagnoses, treatments and outcomes recording. The three have redundancy and problems with incompatible, older computer software architecture. A large group of nursing informaticists is working in the “Vocabulary Unification Summit” to unify and modernize the three code sets into a single well-designed code set for computerizing nursing processes. (Ozolt J, et al, 2001) In 2006, this effort is being assisted by the LOINC committee.

Therefore, in 2006, the situation is being addressed as rapidly as possible by standards-setting groups that are working to finalizing “standard” clinical vocabularies (LOINC, SNOMED), nursing code sets (DHHS, 2002), medical document formats and data element coordination. (CCHIT ref). So many standards development efforts are underway by so many different organizations, that a national Office of the National Coordinator for Health Information Technology (ONCHIT) was established in late 2004. (AAP, 2005) (DHHS, 2005)

Non-HIPAA “Standards”

Some “standards” used in healthcare were not defined under HIPAA. These include:

- 1) Open Database Connectivity (ODBC), is a standardized API (Application Programming Interface) that is a set of programs based on the SQL (structured query language) Access Group (SAG) function set for retrieving data from a SQL database system. ODBC provides very useful access to nearly all modern database management systems and is the most widely supported portable database access method available. But while its name begins with open, implying that it is not tied to a single vendor, in fact, ODBC is controlled by a single vendor, Microsoft. Currently, ODBC is the “defacto”

standard for managing healthcare database queries, and is considered by many to be a database management “standard”.

2) Digital Image Communication (DICOM) is a global information technology standard that was developed by radiologists in 1993 to facilitate electronic transfer of radiologic image files. The DICOM “standard” is copyrighted to the National Electrical manufacturers Association, and maintained by the DICOM standards working group. DICOM is also an International Standards Organization (ISO) standard. This specialized computer communication standard’s committee actively works with the HL7 standard group and uses relevant parts of other standards such as LOINC, SNOMED, TCP/IP and JPEG.

3) Extensible Markup Language (XML) is a structured format that was created to store and send communication that is independent of operating systems and hardware, making it an important tool for transferring data across different computer systems. The standard is maintained by the World Wide Web Consortium W3C, and is especially useful for moving and archiving text-based information across computer systems. The HL7 standard group and the W3C actively work together.

HIPAA Mandates: Privacy “Standards”

Before HIPAA, legal protection of patients’ privacy and confidentiality was fragmented across state, federal and commercial insurance systems, which left many gaps in patient privacy. (Hebda, Czar, and Mascara, 2001; DHHS, 2001) Evolving, implementing and testing patient privacy rules under HIPAA law is an ongoing process. The law is evolving. As early court cases point out, unresolved issues, inconsistencies, and oversights exist in the original law. (Murray, 2005)

HIPAA Mandates: Security “Standards”

Security regulations (“standards”) under HIPAA refer to technical protection of computerized personal health information (PHI) that is transmitted electronically by provider and payer organizations. Security “standards” have three categories: 1) administrative security, e.g. access controls, audit logs and employee training; 2) network or technical security mechanisms, e.g. authenticating users and monitoring user’s actions; and 3) physical security that addresses the actual computer equipment and buildings that house the hardware. (Hirsch, 2003).

For clinical users, the HIPAA law and it’s mandated “standards” have created a very tenuous balance between security and usability. (Dawes, 2001) In practice, legitimate clinical users experience practical problems with passwords, time limitations on the retrieval of records, timeout frustrations with computer terminals, and long access delays caused by need for security logs of all transactions and inquiries to every different part of poorly integrated hospital or healthcare enterprise information systems. The new “standard” security policies and procedures can limit information sharing capabilities in ways that may adversely impact patient care, when applied rigorously by hospital IT departments not focused on clinical usability. Hence, discussion of this set of “standards” is often legally and practically quite contentious, especially when patients call lawyers and/ or IT administrators attempt to sanction clinical care providers.

Think about which “standards” apply when, for example, lab report access is closed at patient discharge, handicapping caregivers who must call parents about late-coming important results (e. g positive cultures, state screen results, bilirubin), or for daily aftercare for ongoing conditions. If there is no parallel paper system, the clinician may never see the critical results. The clinician may also be unable to access the parents’ (or patient’s) contact information. Risk for errors of oversight,

omission and lack of timely communication with parents/patients can be drastically increased when security “standards” are applied too stringently.

So which “standard” are we talking about now? Confusing? You bet.

Necessary? Well, is the automobile necessary?

THINK.

References

- AAP Division of Health Care Finance and Practice. (2005). Alphabet soup: Making sense of acronyms used by electronic health record organizations. American Academy of Pediatrics News, 26(6), 14.
- The Accredited Standards Committee (ASC) X12 (2005). About ASC X12. Retrieved January 9, 2006, from <http://www.x12.org/x12org/about/index.cfm>
- Certification Commission for Healthcare Information Technology <http://www.cchit.org/>
- Dawes, B. (2001). Patient confidentiality takes on a new meaning. AORN Journal, 73(3), 596, 598, 600.
- DICOM – Digital Image Communication in Medicine <http://medical.nema.org/>
- Friedrich, M. J. (2001). Health care practitioners and organizations prepare for approaching HIPAA deadlines. Journal of American Medical Association, 286(13), 1563-1565.
- Health Level Seven (HL7) (2005). What is HL7? Retrieved January 9 2006, from <http://www.hl7.org/>
- Hebda, T., Czar, P., & Mascara, C. (2001). Handbook of Informatics for Nurses and Health Care Professionals (2nd ed.). Upper Saddle River, NJ: Prentice Hall, Inc.
- Hirsch, R. (2003). On HIPAA-The HIPAA Security Rule. Healthcare Informatics, 20(4), 56.
- IEEE Computer Society <http://www.computer.org/portal/site/ieeecs/index.jsp>, and IEEE Internet Protocols http://en.wikipedia.org/wiki/Category:IEEE_802 (Both Retrieved January 9, 2006)
- Linderg, D.A.B., (1987). NLM long range plan. Report of the Board of Regents. Methesda, MD: National Library of Medicine.
- Logical Identifiers Names and Codes (LOINC), Retrieved January 9, 2006 from <http://www.regenstrief.org/loinc/>
- Miriam-Webster OnLine, Retrieved January 9, 2006 from <http://www.m-w.com/dictionary/standard>
- Murray, RBJ. (2005). The subpoena and a day in court: guidelines for nurses. Psychosocial Nursing Mental Health Services,43(3):38-44.
- Office of the National Coordinator for Health Information <http://www.hhs.gov/healthit/>
- Ozbolt J, Androwich I, Bakken S, Button P, Hardiker N, Mead C, Warren J, Zingo C. (2001). The nursing terminology summit: collaboration for progress. Medinfo.,10 (Pt 1):236-40.

T:\Corporate\HHS ONC HITECH\Task 17 FACA\FACA\FACA Meeting Materials\2011-1-10 to 11 Implementation WG\Originals\drummond-imwg-11011.doc

SNOMED International, Retrieved January 9, 2006 from <http://www.snomed.org/>

United States Department of Health and Human Services (DHHS). (2000, last updated). Frequently Asked Questions About Electronic Transaction Standards Adopted Under HIPAA. Retrieved January 9 2006, from <http://aspe.hhs.gov/admsimp/faqt.htm#whynational>

United States Department of Health and Human Services (DHHS). (2001, May 9). Protecting the privacy of patients' health information. Retrieved January 9 2006, from <http://aspe.os.dhhs.gov/admsimp/final/pvcfact2.htm>.

United States Department of Health and Human Services (DHHS). (2005). Office of the National Coordinator for Health Information Technology (ONC). Retrieved January 9 2006, from <http://www.hhs.gov/healthit/>

United States Department of Health and Human Services (DHHS). (2002, May 31). Health Insurance Reform: Modifications to Electronic Data Transaction Standards and Code Sets (45 CFR Part 162)

XML <http://healthcare.xml.org/>

<http://www.w3.org/XML/>

<http://www.w3.org/Consortium/>