



Standards Insight

An Analysis of Health Information Standards Development Initiatives

August 2002

This information, prepared as a benefit to HIMSS members, is **not** for public distribution. Parts may however, be incorporated in internal and external communications. Attribution as to source is appreciated. Your comments on this publication and HIMSS' standards development analysis reporting efforts on your behalf are valued.

©Copyright HIMSS, 2002. All rights reserved.

Table of Contents

Introduction	2
Business Requirements	2
Why Interoperability?	2
Supply Chain or Value Chain	5
An Aside on Capital Budgeting.....	6
Interoperability and Web Services	6
Inside the Firewall.....	6
The Cost-Benefits Outside the Firewall.....	6
The Business of Standards.....	7
Politics and Business Interests.....	7
National and International Standards	7
Standard Code Sets.....	8
SNOMED	8
Summit on Nursing Terminology.....	9
NAHIT	9
Bottom Line.....	10
Next Issue	10

Introduction

The *Standards Insight* is a bi-monthly business review of interoperability initiatives for HIMSS members. The *Standards Insight* is a business not a technical review. It presents a management viewpoint of how to use interoperability standards to meet an organization's business requirements. Business is thus a comprehensive, but imprecise, umbrella term. However, we also apply the term "business" to processes that include both the back-office functions of healthcare organizations and also the clinical processes – the real "business" of healthcare. Finally we use the term "business" interests to convey the concept of economic analysis and, in some cases, commercial motives. Thus the *Standards Insight* is a management review of interoperability standards for the purpose of understanding what business requirements they address, how they impact business functions and processes and whose business interests they reflect.

In this issue we will expand on the relationship between business requirements and systems interoperability standards. We will look at a corollary relationship between business interests and standards developers. In the course of this discussion, we also will report on several standards initiatives, including the US Technical Advisory Group to ISO Technical Committee 215 (healthcare informatics), SNOMED and the National Alliance for Healthcare Information Technology (NAHIT).

Business Requirements

In the last issue, we discussed the value of establishing business requirements for interoperability standards. We did this in the context of the then upcoming meeting of the National Alliance for Healthcare Information Technology held June 25th in Washington, DC. The NAHIT is an ad hoc industry consortium called by the American Hospital Association (AHA). A report on the NAHIT is included later in this issue.

Dick Davidson, the president of AHA, described the AHA's motivation for calling for this coalition by recalling that, in developing the AHA's strategic plan for reforming health care, the industry group has highlighted six (core initiatives):

- Providing coverage and access
- Insuring patient safety and quality (reducing errors)
- Sustaining their workforce (ameliorating the nursing shortage)
- Gaining regulatory relief (from HIPAA)
- Improving payments (again HIPAA)
- Preparing disaster readiness plans

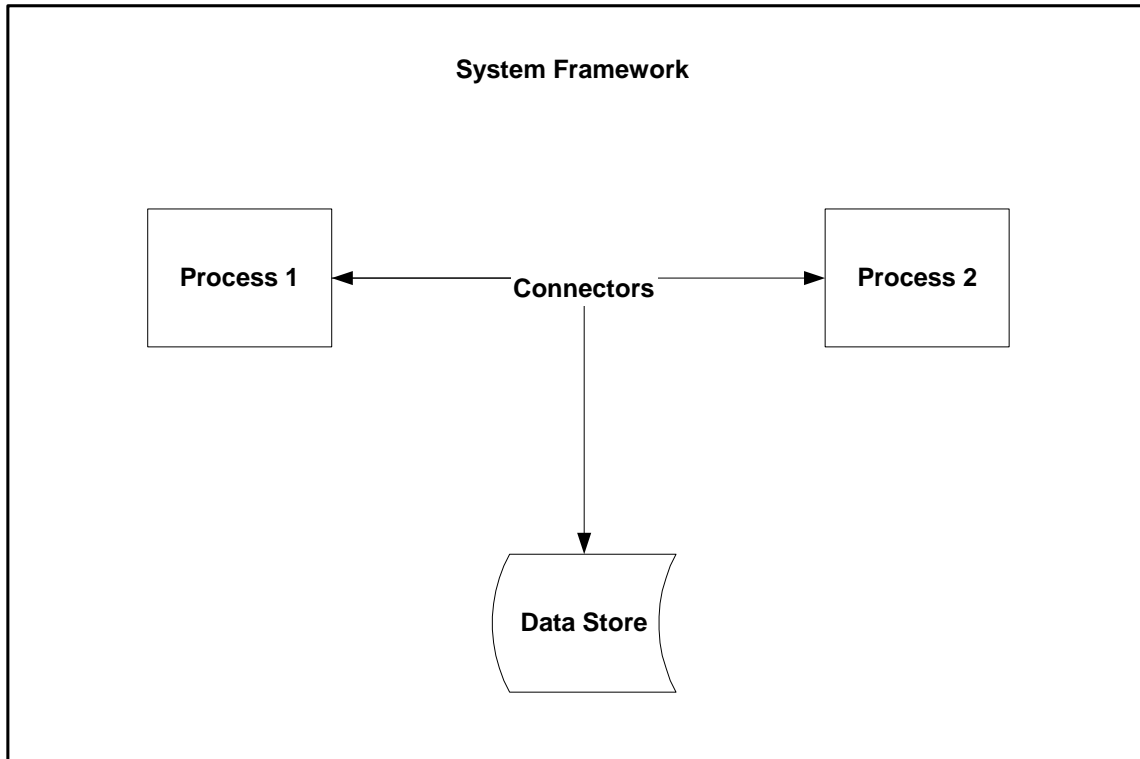
The AHA concluded that IT was an essential enabler in addressing all of these issues, and that IT requires interoperability standards to be effective and efficient. This is a clear statement of business requirements that reflect the business interests of the AHA and the other NAHIT members in seeking to promote key interoperability initiatives. It also points out how IT enables health care in a ubiquitous manner unlike any other technology.

Why Interoperability?

Like the AHA, we all start from a bias that automating business (care) processes is good but that islands of automation are bad; thus interoperability is necessary, and achieving interoperability depends on standards. At their core these are valid beliefs, but we need to carefully examine each. Business requirements should drive business process improvement and automation initiatives. In fact much of the current emphasis on improving care processes and outcomes is a business initiative – based on an evaluation of value produced for resources consumed. From this premise concerning business requirements, we derive the other three beliefs based on high-level system design principles. In fact we have enunciated four core elements of a systems model:

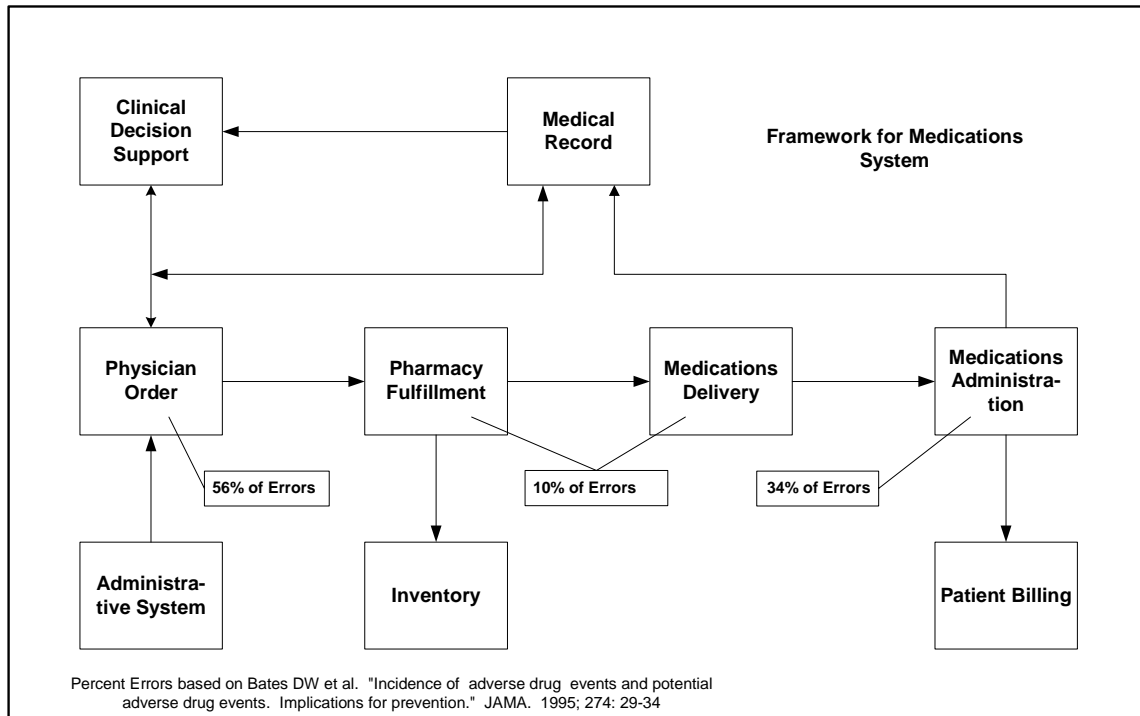
- A framework to organize the system's scope and components

- Key business processes automated through different applications
- Connectors to enable the processes and applications to interoperate and share data
- A special process to permanently store the record of key processes, results and outcomes.



In this simple model, we should point out that we spend most of the IT budget on the applications that automate the processes. However, it is really the framework that is aligned with business requirements and the connectors - the realm of interoperability standards - that create the system.

For example, we might consider the system required to automate the process of providing medications to inpatients. Automating pharmacy functions has long been a business practice in larger hospitals. Adding a medications administration function has been shown to reduce errors and improve patient care. Separately automating physician order entry and providing decision support also can reduce errors and improve patient care. Each system, as an independent island of process automation, can achieve its immediate business objectives. However, by making these three systems interoperate we can reduce redundant, error prone and untimely manual data entry and generally improve the overall process of care. Moreover, we gain further "business" efficiencies by linking this medications system to patient billing and inventory management systems. From a common hospital process of providing medications to a patient, we have created a complex system of different functions and applications, each with different purposes and potentially different terminologies.



We might accomplish such interoperability by purchasing an integrated solution from a single vendor. Although there might be such solutions for this example, in the end we will not be able to find or be satisfied with a single vendor solution for all automation in an enterprise, let alone across all healthcare enterprises. We prefer open systems that enable us to choose the best modular solutions at a given time. Moreover, few organizations could afford a new completely integrated system given their investment in legacy systems. We will always be faced with a need for incremental transitions. Thus, we develop the case for interoperability standards to permit different systems to work together as modules incrementally implemented over time.

Interoperability, to most of us who have grown up in the industry, has meant messaging interfaces between internal systems. Data from one application was sent to another. The messaging format was defined although content itself was not. In most cases, these were implemented through interface engines that could do some transformations, but analysts still needed to map data content from one application to a common library. External interoperability was based on batch file transfers or electronic data interchange (EDI) based on bilateral (really unilateral) specifications.

More recently interoperability has come to encompass a much broader spectrum of attributes. We often use interoperability to mean system integration, for example. In turn, system integration can take place at multiple layers from physical networking to data to applications. Enterprise application integration (EAI) evolved to encompass a broader set of services than standard message translations including standard terminologies and appropriate event driven actions. Moreover, such interoperability often is assumed to be in real time, a zero latency system – certainly not an old-fashioned batch processing system. Finally, our expected scope of interoperability has changed. Everything should work with everything else. Enterprise resource planning (ERP) moved beyond supply chain management to operational management systems.

The Web helped change our concepts of interoperability. Several years ago, as the Web and Internet emerged as the dominant focus of IT, industry rushed to embrace the potential of external (to the enterprise) interoperability – the world of B2B and B2C. Because the Web promised to make it “easy,” we extended the concept of system interoperability from systems inside the enterprise to those outside the enterprise. Web services¹ were originally perceived as a means to dynamically interoperate between enterprises – a replacement for EDI. For example, we saw the growth of ebXML to show how to combine Web services including repositories, trading partner agreements and messages to conduct e-commerce.

Healthcare was no different, as hospitals went through steps of creating Web sites, providing physician portals, and linking themselves to their “partners.” IT enabled the technology, not the business requirements, to define the problems. Thus, we focused on using Web technologies to link to our external partners. We confused the supply chain for the value chain. We let the technology define the problem rather than asking what business problems the new tools could solve.

However, we now are seeing corrections within the IT world as Web services are becoming more directed at internal systems because that is where one will find the greatest business leverage. For example the mission of the Web Services Interoperability Organization (WS-I) is to show enterprises how to use and combine Web services, such as SOAP and UDDI, within the enterprise. That such distributed services are built on Web technologies will make it much easier to move from within to outside the firewall – when the business case is made. This is a key lesson for us within healthcare; we should design our systems, and our interoperability standards from the inside out, not from the outside in.

In the past 15 to 20 years, healthcare information interoperability standards have advanced from a relatively simplistic high-level view of a series of hospital computers sending basic data messages to each other towards a loosely coupled system of interoperating computers within and without the enterprise.

Supply Chain or Value Chain

Michael Porter originally described the “value chain” in his 1985 text *Competitive Advantage*.² At its basic level, the value chain described the activities within a firm that created value and competitive advantage. He went on to describe a value system in which upstream and downstream firms were included. However, unless a hospital is only a purchasing department and a billing office, the essence of value chain is what the hospital adds to patient care, not how low its inventory costs are or how quickly it can send out a patient bill. Moreover, while hospitals do use a significant amount of expensive drugs, supplies and devices “the inbound logistics” in Porter’s analysis - “outbound logistics” are not generally how we refer to discharged patients. Yet because IT and the Web offered the tools for enterprise resource planning and supply chain management, we embraced the concept. After all, Arthur Andersen estimated the gains from the healthcare e-chain to be approximately \$6 billion to \$7 billion a year. Our current experience with HIPAA administrative simplification is based on an estimate that, by the tenth year, the healthcare industry will save \$5.6 billion a year. These are large numbers to be sure and worth pursuing.

However, healthcare spending has exceeded \$1 trillion a year. Hospitals spend more than \$400 billion a year. The supply chain and HIPAA net savings to hospitals, in the best case, represent about \$5 billion a year or 1 percent of total expenses.

¹ Web services have been defined as XML objects (or components that contain data and logic) that are accessed over TCP/IP networks using SOAP.

² Michael Porter. “Competitive Advantage.” Free Press. New York. 1985

More than half of hospitals' total expenses are for labor, a figure that would jump to 60 percent if physician services provided in hospitals were included. It is the organization, delivery and management of caregivers that produces the added value in healthcare. The best medication from the best pharmacy inventory, wrongly administered, does not produce value. The value chain for healthcare is not equivalent to the supply chain.³ IT uniquely among medical technologies provides leverage for all care providers. Whereas some technologies, such as diagnostic scanners or lasers or breakthrough drugs enable superior outcomes for some patients, IT can enable improved care for all patients. Conversely, inadequate systems are the source of or major contributing factor to most medical errors. We also should note that we have referred to such care management systems as clinical information systems, not enterprise resource planning systems. This perspective will be useful in establishing priorities for interoperability standards. Thus, we return to the issue of business requirements driving IT interoperability requirements.

An Aside on Capital Budgeting

In the normal course of capital budgeting, one would expect that projects with the highest return on investment and highest strategic value to be approved down to the point of projects whose return on investment (ROI) was no greater than the cost of capital. While this is generally true in health care, there are two other factors that are involved. The first is that many patient care initiatives, such as computerized physician order entry (CPOE) or medication administration, are perceived to have "soft" dollar paybacks in comparison to "hard" dollar savings, such as lower supplies costs. Somehow, the tools of "business" analysis do not work as well with clinical activities and outcomes. Second, hospitals, particularly not-for-profit entities, have a limited ability to raise capital, even for projects with positive ROI. This creates a bias to undertake projects that have short paybacks in measurable dollars. This may explain why there has been such attention provided to external financial and supply systems and not internal clinical systems. The value chain makes the argument for focusing IT investment and interoperability on internal clinical processes while the supply chain looks to external processes. Actually a short-term focus, i.e. an incremental or modular approach to systems, appears to work much better than "big bang" major IT projects. The determinant of success is whether the incremental projects are within a strategic framework that reflects the directions and priorities of the organization.

Of all objectives that the NAHIT could accomplish, establishing the business requirements for clinical interoperability – backed by the market driven commitment of their members – would be the most significant.

Interoperability and Web Services

Inside the Firewall

If we believe that it is the caregivers and their support systems within a healthcare organization that define and produce the essential value of the organization, it stands to reason that this is where IT has the highest leverage. Our awareness of the costs of medical errors, essentially an internal human and systems problem, has risen dramatically with the reports from the Institute of Medicine and the Leapfrog initiative.

As this year's HIMSS Leadership Survey illustrates, our IT focus is on improving clinical processes. We all understand that clinical data is the source data for healthcare systems. Moreover, it is difficult to make it more accurate, precise or secure upstream from the point of care. This implies the importance of clinical interoperability standards to support these initiatives. Interoperable clinical systems, not supply chain systems, have the higher priority because that is where the real leverage of IT resides. Cutting costs without managed processes may produce the expected 1 or 2 percent savings but will fail to impact outcomes or provide a superior competitive position. Perversely, we are spending our IT dollars on financial systems interoperability.

The Cost-Benefits Outside the Firewall

³ For further discussion on the healthcare value chain and supply chain refer to Lawton Burns and Wharton School Colleagues. "The Health Care Value Chain." Jossey-Bass. San Francisco. 2002

Venturing beyond the firewall does produce benefits of course. While managing the supply chain may not be at the center of the value chain, there are benefits – although most of them accrue to the external partner. Connecting with patients and consumers is a high priority for all healthcare organizations. Public health services and clinical research trials produce large benefits for society and to future individual patient care.

However, there are two significant costs that jump when one goes beyond the firewall: interoperability and security. In the last issue, we described how business issues overtook the purely technical issues in terms of costs and complexity after we venture there. More specifically, the business issues arise from security and interoperability requirements after a single entity no longer controls the system. If one has an internally secure and interoperable system, the technical costs of extending the system beyond the firewall are not as great as the business costs of managing security and mapping multiple systems. In fact, while both interoperability and security increase costs and complexities, they have a synergistic effect. The more one wants interoperability, the higher the security costs are. Security adds an added layer of complexity to interoperability. Security limits access while interoperability provides access. This leads to the key questions beyond the firewall: who pays and who benefits? For example, public key infrastructure (PKI), a technically robust inter-enterprise security framework, is not viable because of the business costs of administering the system.

The Business of Standards

We describe interoperability standards in terms of being open and technology neutral, as the result of a consensus process. In fact most standards are not open, free or neutral. They are the product of competing political and business interests of the parties participating in the effort.

Politics and Business Interests

Most of the key issues and impediments in standards development are not technical issues, at least not technical issues unassociated with business interests. Business interests seek to gain competitive advantage or advance a particular technology or solution. In selecting one model or technology for a standard, a Standards Development Organization (SDO) rejects other approaches and is conveying something of a monopoly. Business interests are not bad – they justify the resources to get things done. However, business interests must be balanced in standards development whether through voluntary consensus or regulatory due process.

We have described the process of voluntary consensus standards development in previous issues. In general, this method requires much front-end discussion and issue resolution to reach consensus. Those who prevail are those that do the work – such volunteers represent interests that pay for this effort. In that sense, standards are not free, open or neutral but the product of funded interests participating in a defined process to see their position prevail. Commercial self-interest is on an equal footing with academic worldviews.

National and International Standards

Perhaps the issues of politics and interests in voluntary standards development initiatives are nowhere more evident than in the international standards development arena. The US Technical Advisory Group to ISO Technical Committee 215 (healthcare informatics) is the official representative of the US position at ISO.⁴ The US TAG does not develop standards. It is the conduit for US SDOs to advance national standards to international levels.

⁴ Further complicating the politics and interests is the fact that the US TAG's secretariat is ASTM, not ANSI. The ANSI Healthcare Informatics Standards Board (ANSI HISB) is responsible for coordinating US healthcare SDOs but not their positioning within the world community, while the US TAG does the positioning without coordinating.

The United States healthcare information systems market is 40 to 50 percent of the world market. Historically healthcare information systems (HCIS) products have not traveled well beyond national borders primarily because the administrative and financial processes that they address are different from one country to the next. This market isolationism is changing rapidly, as clinical information systems become the focal point. In July, the US TAG conducted an open meeting for any interested party in an effort to get wider participation. It worked on developing US positions for electronic medical records, population models, security frameworks, smart cards and wireless networking. Whether the US position represents our interests, whether it prevails as an international standard or whether it makes a difference in any event do not appear to be matters of great concern to the healthcare industry, based on the level of participation in the July meeting.

Standard Code Sets

We have described our interoperability standards as the lines connecting the processes. To insure interoperability, the standards must define the message format, usage, context and content. Within the firewall in the world of clinical systems, Health Level 7 (HL7) has emerged as the primary source of message format and context standards. Context can be seen in terms of data containers, such as documents, and rules for messages, i.e. trigger events. However, HL7 does not address content at the vocabulary or code set level. Instead, it uses profiles to register and reference external code sets and/or mappings.

A controlled vocabulary, as Gartner and SNOMED point out, is essential to an electronic medical record. However, we should understand the difference between adopting a single standard code set and having a common standard code to which to map. The former represents an enormous technical and cultural challenge while the latter is a doable task, whether through language engines or Web services. Moreover, one aspect of Web services that supports dynamic discovery and repositories lend themselves to local code sets that are mapped to a standard reference set. Virtually all clinical data, the source data for all systems, is created and used within an organization. One of the costs of going beyond the firewall is to map that data to other standards.

SNOMED

Of the various clinical code sets available, SNOMED is probably considered the most complete and descriptive. SNOMED International, a subsidiary of the College of American Pathologists, develops and licenses SNOMED. Although SNOMED International is an ANSI accredited standards development organization, its code set is not yet an ANSI standard.

SNOMED is a concept-based, hierarchical coding system. Terms can be combined to reduce ambiguity. SNOMED CT (Clinical Terms) is a union of SNOMED RT (Reference Terminology) and the Clinical Terms Version 3 (CTV3 or Read Codes) from the National Health Services of the United Kingdom. The latter adds depth in the area of primary care medicine.

While extremely comprehensive, SNOMED still includes some gaps in its own codes. SNOMED uses the LOINC codes for clinical lab values and has mappings to the primary financial and billing codes including CPT, ICD and HICPICS. However, SNOMED does not include nursing terms or detailed drug coding.

SNOMED's effort to become the HL7 of code sets.

Despite its technical strengths, SNOMED's business model has prevented SNOMED from being adopted as the code set of choice. SNOMED is not a volunteer based SDO. While it seeks input from its Clinical Partners Board, it does not use the consensus method to develop its standards. Like the AMA and its CPT codes, SNOMED depends on licensing fees to support its own development efforts. Such funding, supplemented by the CAP, permits predictable staffing and project plans as well as consistent and coherent releases.

It is the licensing fees and lack of open consensus that has generated resistance to SNOMED within the healthcare community. Pricing is a real as well as perceived problem. Generally, the annual licensing fee is value-priced based on volume. If a vendor builds SNOMED into its applications, it pays a license fee as does the end-user. End-user licensing becomes complex as multiple applications, each incorporating SNOMED, are implemented.

International scope

While SNOMED has strengthened its code set by adding CVT3, it has also greatly expanded its problem set. It must meet the needs of both the US and the UK. While basic clinical concepts may find common acceptance worldwide, detailed codes involving subspecialty procedures, drugs and nursing will not travel as well. In addition, multiple mappings to other administrative and financial code sets will be necessary. Like HL7, having international scope strengthens the ultimate product but will complicate and slow development.

Summit on Nursing Terminology

The July Summit on Nursing Terminology is a good example of the approach of using domain specific code sets mapped to a reference terminology. The nursing community long has used its own terminologies for describing nursing diagnoses and procedures. Many are similar to terms physicians use, some are more detailed, and some are specific to the nursing role. Moreover, nursing itself used different code sets within its own domain. One might suppose that since nursing procedures were not a billable item, there was no external body to compel single standards as with physician procedure codes. However, the nursing community recognized the need to standardize its own terms and link them into standard code set, i.e. SNOMED, so that they might be used as part of a standard electronic medical record. In the July summit, they proposed a plan for Nursing Reference Terminology Model. It is a good four-step model for evolving a standard code set.

- Develop and inventory one's own terminologies and codes
- Map these to a "standard" terminology, like SNOMED
- Find and fill holes
- Converge over nursing terminology to standard over time

NAHIT

The AHA hosted a recruiting meeting for the National Alliance for Healthcare Information Technology in Washington on June 24. The meeting was well-attended, with participation by industry and vendor corporate executives, lobbyists, consultants, government officials and others. As a recruiting meeting, it had to be judged a success - by the end of the day, there were 35 founding members signed up, and that list has risen to 72 members to date.

Substantive discussions of objectives, organization and programs were deferred to an August meeting. Thus, the direction of NAHIT is unclear and, presumably, it is still open to be shaped.

The one action that did emerge was the NAHIT decision to develop and present a position on bar coding at the July 26 FDA hearing. Reports from the hearing indicate that most presenters were in favor of FDA action and that the FDA generally is willing to require drug manufacturers to put bar codes on all of their unit-dose packaging. However, as we know from HIPAA, asking the Federal government to publish regulations to solve a problem that industry cannot do on its own leads to unforeseen consequences. Regulations have the potential to promote and to delay. First and foremost, it will freeze any bar coding initiatives and investments as we await Federal rules. Second, the economics of bar coding are significant and it is not clear who pays. If pharmaceutical manufacturers are required to put bar codes on unit doses, will some reduce their unit dose offering? What will be the requirement on hospitals to use the bar codes? At the least, a potential legal liability is created if a hospital elects not to use the bar codes. Some estimates indicate that the cost of implementing bar coding and related computer systems at the point of care will be \$1.5 billion. While the payback in reduced errors and better processes and outcomes

should provide ample payback over a few years (there does not appear to be any incremental payments from the government or insurers), these tend to be the soft dollars that hospitals have trouble justifying. So will bar coding become a regulated requirement moving to the head of the capital budget line – perhaps in place of CPOE, which potentially will reduce errors by two times the amount?

We do know that the bar codes standards themselves are only part of the interoperability issue. To provide the foreseen benefits, all the interoperability described in our earlier example must be in place. Interoperable standards will be needed to integrate NDC numbers, dose, routes of administration, lot numbers and expiration dates into the multiple processes from physician ordering, dispensing and inventory, delivery and administration, and finally billing.

Bottom Line

Interoperability standards are an important component of any information system. The more complex and complete the system, the greater the importance of interoperability between processes and applications. Yet as an industry, we put considerably less time and resources into planning, developing and evaluating interoperability standards than we do applications. We need to set business priorities and directions – not let technology set investment agenda. We would not want our clinical processes based on ERP or our clinical codes on Medicare billing terms. We would not want our system security based on external system needs. Our standards should reflect our value chain not our supply chain. They should permit maximum flexibility in modular and incremental implementations. While mapping to a single terminology is valuable, a single terminology cannot replace the rich set of codes used in different domains – at least not immediately. Web services, such as repositories and dynamic discovery, open the technical solution set so we should make sure our business requirements do not presume a specific technical solution.

Next Issue

We note in passing that HHS released the final HIPAA Privacy Rules, which were basically unchanged from the March NPRM. Of greater interest is that HHS again has pushed back the final Security Rules until October. While common wisdom is that they will not change substantially from the 1998 NPRM, except to conform them to the changes in the Privacy Rules, we note in passing that the Federal government will release a cyber-security plan in mid-September. It may require all government agencies to purchase only IT that is certified under the National Institute of Standards and Technology's National Information Assurance Plan (NIAP). The plan includes recommended safeguards for all industries, not just government agencies.

HL7 holds its annual plenary session in early October. We will look again at its role as the premier clinical SDO from a business perspective – how well is it meeting the business needs of the industry?

Please direct any questions, suggestions or comments regarding *Standards Insight* to Joyce Sensmeier (jsensmeier@himss.org) or its author, Ed Larsen (erlarsen@erlinc.com).