



Standards Insight

An Analysis of Health Information Standards Development Initiatives

February 25, 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's standards development analysis reporting efforts on your behalf are valued.

©Copyright HIMSS, 2002. All rights reserved.

Table of Contents

Introduction	2
HIMSS 2002 and an overview of HCIT	3
Bioterrorism.....	3
Interoperability at intersection of business and IT plans.....	3
Computerized physician order entry and CIS.....	3
Enterprise resource planning (ERP) has also grown sharply in importance.....	5
Interoperability demos	5
HIPAA "Compliance" Update - the current big thing.....	5
Phoenix Health Systems/HIMSS Quarterly Survey.....	5
Complying not leveraging	6
Claims attachments	6
Privacy is doable.....	7
Security is the biggest issue.	7
The Porter report	8
Interoperable security systems - end-to-end	8
An E2E Security Framework	10
HL7 Winter Working Group – January 2002.....	11
Overview.....	11
Version 3.0 Update.....	12
The Clinical Document Architecture	13
Security in HL7	13
Next Issue	14

Introduction

The *Standards Insight* is a business analysis of healthcare interoperability standards initiatives provided to all Healthcare Information and Management Systems Society (HIMSS) members.¹ Interoperability standards are essential to both end-users and vendors to enable different systems and applications to work together. Such standards are the product of voluntary standards development organizations (SDOs), such as HL7 or ASC X12N, of federal mandates, such as the HIPAA transactions and codes, and of ad hoc efforts such as Integrating the Healthcare Enterprise (IHE).

In our first issue in December 1999, we described the tension among various standards development and acceleration initiatives competing for domain and scope. We laid out the proposition that standards initiatives can be evaluated in both technical and business terms. Such analysis is useful to management in deciding which standards to support in developing or purchasing new applications. Technical aspects include a standards' completeness based on its role, its specificity (plug and play), and its compatibility with other standards. The business aspects, how successful the standard and its organization will be in gaining acceptance, include the breath of participation, resources, and critical mass in the market. We identified HL7 (the clinical domain, with international scope and wide market acceptance), ASC X12N (in the financial domain, a US focus with its managed-care transactions mandated by HIPAA), DICOM (its domain limited to imaging, international in scope and wide acceptance within its segment), and NCPDP (pharmacy-based prescriptions within the United States), as the most important standards initiatives.²

In a just completed survey of HIMSS member, respondents listed HL7, ASC X12N, EDIINT, IHE, and DICOM as the standards initiatives of highest interest to them. The HIMSS respondents also listed the standards issues that they most wanted addressed:

- HIPAA Security
- Electronic Medical Record
- Digital/Electronic Signature
- HIPAA Privacy

We believe that the *Standards Insight* is aligned with these initiatives and issues. However, we welcome any input, comments, questions, or alternative views from all HIMSS members. See the last page for contact information.

In this first issue of 2002, we use the HIMSS Annual Conference and Exhibition as a vantage point to survey the industry and give perspective to interoperability. This will lead us to an update on HIPAA³ standards, particularly security. Finally, we will review HL7 and its recent winter working group meeting.

¹ The *Standards Insight* had been published bi-monthly by the Center for Healthcare Management (CHIM) for its corporate members. Effective January 1, 2002, CHIM reunified with HIMSS. HIMSS is making the *Standards Insight* available to its members. All 2001 issues are available on the individual member home page at www.himss.org.

² Last year, the National Committee on Vital and Health Statistics evaluated the suitability of existing standards as the basis for HIPAA "recommended" standards for their patient medical record information project. NCVHS is currently preparing a recommendation for HHS that HL7, DICOM, and NCPDP standards be adopted in their respective core and segment domains.

³ We use HIPAA loosely to mean the Administrative Simplification provisions.

HIMSS 2002 and an overview of HCIT

The war on terrorism and homeland security have caused all of us, including executives and boards of healthcare organizations, to re-evaluate plans and priorities. In a recent *HealthLeaders* poll, HIPAA, staffing shortages, reimbursement, and terrorism preparedness were identified as the biggest challenges facing healthcare in 2002.⁴ The just-completed 13th Annual HIMSS Leadership Survey found that HIPAA compliance, controlling costs, gaining operational efficiencies, and reducing medical errors were the top business priorities. Reducing medical errors showed the sharpest increase from the prior year, leaping from 31 percent to 44 percent agreement. Interestingly, this is almost equal to the decline in improving operational efficiencies. Might the former be a better way to accomplish the latter? One can discern that HIPAA focus has shifted to security and that medical error reduction is part of a pattern of improving processes and reducing costs. These priorities are the result of management decisions, not IT preferences or government mandates.

It should also be noted that the slowing economy and double-digit increases in healthcare costs will force a new strategy for controlling healthcare costs. Perhaps the Leapfrog initiative may emerge as a successor to managed care. In the meantime, the better operating margins that hospitals have been experiencing due to Balanced Budget Act givebacks and improved contracting are the seeds of the next round of tightening. Eventually, this will work back into IT spending plans.

Bioterrorism

We also note parenthetically that Bioterrorism was a featured topic at HIMSS. One of the reasons that HIPAA has become relatively less important to HHS is their growing focus on Bioterrorism and public health responses. While there is a rudimentary national reporting network, it is not automated or interoperable. This may lead to stovepipe solutions because a national healthcare infrastructure (HIPAA 2) does not exist. Homeland security will channel HCIT efforts and priorities, but as yet, in unclear ways.

Interoperability at intersection of business and IT plans

Changing healthcare business priorities are shaping HCIT plans. The HIMSS Leadership Survey found that upgrading security/HIPAA compliance, reducing medical errors, and upgrading inpatient clinical systems were the top IT priorities near- and mid-term. Thus, there is some alignment of business and IT plans. We make the point that none of these or other top initiatives can be achieved without interoperability.

Computerized physician order entry and Clinical Information Systems (CIS)

Before we update HIPAA, we should look at computerized physician order entry (CPOE) and clinical information systems, which are the next big things after HIPAA. The dominant theme at HIMSS 2002 was reducing medical errors, improving clinical processes, and operational efficiencies. The "hot" technology was computerized physician order entry.

The Institute of Medicine studies on medical errors and fixing the system have had a major impact on healthcare organizations. However, it is the Leapfrog Group that has made these a high-profile business issue. Leapfrog is a loose association of public and private purchasers, many of the Fortune 50, as well as Blues, states' Medicaid agencies and, potentially, the Centers for Medicare and Medicaid Services (CMS).

Leapfrog has focused on the costs and poor quality that results from medical errors and process variance, including the controversial 44,000 to 98,000 avoidable hospital deaths per year. It has applied industry lessons in process control and quality analysis to healthcare. Rather than getting into detailed recommendations, such as the 78 process improvement recommendations from the University of California, Leapfrog chose three, high-impact proxy measures for best practices:

⁴ Results posted January 22, 2002 at www.healthleaders.com.

- Computerized physician order entry
- Full time intensivist supervision of critical care
- Minimum annual number of seven high-risk procedures

Leapfrog leaves it to the healthcare providers to figure out how to improve their own support systems and processes to meet these objectives. If they can deliver, Leapfrog will make their quality measures essential to a provider's market viability.

The impact of Leapfrog and other quality initiatives on HCIT will be to drive integrated clinical information systems, not just computerized physician order entry.

One cannot implement an effective computerized physician order entry system without a clinical information system. At a basic level, it is unlikely that physicians will use computers to enter orders when all the data they depend on, such as lab results, charts, current medications, etc., are in paper form. Secondly, unless all the clinical data is in the "system," the CPOE module cannot apply rules to detect contraindicated orders. Finally, without an integrated CIS, one cannot close the loop through the pharmacy to medications administration to reduce all medication errors. We also note that CPOE does not eliminate all medical errors or causes of variance.

Thus, the Leadership Survey notes that clinical information systems, point-of-care decision support, the Computer-based Patient Record (CPR), and Clinical Data Repository (CDR) have all risen (compared to 2001 results) in importance as applications to be addressed over the next two years. Of course, an integrated CIS with CPOE requires interoperability, whether between different vendors' systems or even within a single vendor's system.

Leapfrog stands in contrast to HIPAA as a model for change

HIPAA Administrative Simplification has been presented as a means of doing with regulation what the healthcare industry could not do for itself voluntarily; adopt cost-savings standards for patient billing and related electronic transactions while protecting the privacy and security of patient data. It imposes detailed federal regulations and penalties to accomplish its ends. It consists of hundreds of pages of comments interpretations, discussions and, of course, rules in the Federal Register. It is six years in the making and still not final. It has frozen new technology initiatives, such as XML, and failed to solve technical issues such as electronic signature. Change and clarifications are slow in moving through the Federal bureaucracy.

In contrast, Leapfrog is three years in the making. It seeks to use informed consumers and market pressure to force healthcare providers to improve their processes and systems to meet key objectives. It requires providers to let it and consumers know how they are doing in moving toward the objectives. It does not tell providers how to accomplish the objectives nor does it establish any dates by which they must be met. In five years, we can look back and see which model was more effective in bringing about change within their respect scopes.

One can argue, as many provider groups have, that the Leapfrog objectives are unreasonable and unattainable. For example, most hospitals in Michigan, could never meet the intensivist or procedure volume requirements even if they could afford CPOE. Rather than question whether there is some better way of delivering care, e.g., consolidating services, the hospitals and their physicians attacked the rules as naïve, reflecting the ignorance of healthcare by corporate executives. In the name of patient safety, the Healthcare Leadership Council, the AHA, and the Federation of American Hospitals sponsored a "study" proposing principles for judging the "standards" to be applied to hospitals. Not surprisingly, these standards had to apply to all hospitals. This appears to be an attempt to water down Leapfrog in the name of equal safety for all patients. As with HIPAA and the disconnect between management and IT, we will have to decide as leaders in HCOs, vendors, or consultants, what interests we serve and what business case can be made to executive management to insure the support of and alignment with the organization.

Enterprise resource planning (ERP) has also grown sharply in importance

While this does not fit neatly into our CIS scenario, it does support the business priorities of reducing costs and increasing operational efficiency. We do not know for sure what respondents to the Leadership Survey meant by ERP, but we will presume that it will have to be integrated with CIS if it is to be successful. Supply chain management, human resources and staffing, asset management and customer relations, the typical ERP suite, are of little value in healthcare organizations unless they are linked to clinical processes and data. Most early adopters have found that there are marginal savings in the stand-alone ERP modules, but drug costs cannot be managed if the system only goes as far into processes as the pharmacy inventory. Staffing productivity cannot be evaluated without understanding the care processes and patient acuity.

Like CPOE, ERP will need to interoperate with the core CIS.

Interoperability demos

HL7 and IHE each presented interoperability demos at HIMSS. HL7 presented a very sophisticated demonstration of broad scope. Seventeen vendors linked a wide range of applications, using both version 2 and version 3 XML messaging the clinical document architecture, CCOW, and HIPAA claims attachments. The demo showed how HL7 can mix and match its standards and applications according to the data needs and capabilities of the participating applications. The scenario included clinical, administrative, and financial operations one might find in or among a major healthcare enterprise. Moreover, the demo used the standards, not hard-wired proxies (which did lead to a significant amount of debugging of the implementation spec.)

In contrast IHE presented an in-depth demonstration of interoperability within an imaging department with select messaging with an HIS. We reviewed the same demo from RSNA in the last issue.

The two demos highlight the difference between HL7 and IHE in achieving plug and play interoperability: completeness versus speed. The former addresses the entire clinical spectrum using a top-down model approach that will automatically derive interoperable messages. The latter is in a limited clinical domain using a bottom-up approach to constrain the implementation of selected DICOM and HL7 messages. One promises interoperability across all clinical systems, the other provides specific operability among imaging systems. In the end, IHE will have to move to HL7 in the enterprise but in the meantime radiology departments can achieve plug and play.

HIPAA “Compliance” Update - the current big thing

The HIPAA news from HIMSS is not surprisingly that it remains the top business and IT priority. According to the HIMSS/Phoenix Health Systems quarterly survey, there is slowing progress to meet dates depending on whom you ask. Large hospitals and health plans are coming along, but other covered parties may be lagging. Implementing the standard transactions and codes is proving more difficult and less rewarding than HIPAA stalwarts had expected. Most healthcare organizations, because of time and money, are opting for remediation and not re-engineering.

Phoenix Health Systems/HIMSS Quarterly HIPAA Survey

Phoenix Health Systems (www.healthadvisory.com), now in conjunction with HIMSS, conducts self-selected surveys of the industry's HIPAA readiness. The surveys are useful in tracking industry trends. January results suggest gradual but slowing progress. The year's delay in requiring use of the standard transactions and codes may be having an effect of blunting perceived momentum. Right now, most organizations appear to be targeting completion dates very close to compliance dates. For example, 70 percent of providers have not finished assessments, although virtually all are expected to be finished by now when responding six months ago. While respondents understand that the delay in transactions and codes does not impact any other rules, i.e., privacy, one can speculate that the delays and/or benign neglect may occur here, too.

A consistent finding of the surveys is that time and budget are seen as the two biggest barriers to HIPAA compliance. However, in the latest survey, problems in interpreting the rules has moved into this grouping. This is a significant finding now that organizations have real experience with assessing and implementing HIPAA rules.

Forty to 50 percent of respondents say that they are implementing HIPAA as part of a strategic initiative with an additional 20 percent indicating greater effort to achieve best practices. Only 27 percent said they were simply doing the minimum to comply. These results do not square with other sources and our experience which indicate closer to 90 percent are only doing what is necessary. This may reflect the self-selection process or a definitional problem.

Complying not leveraging

Most healthcare organizations, we believe, have chosen to view HIPAA Administrative Simplification as new federal regulations to be complied with, not as a strategic opportunity to re-engineer their processes. The executive decision to simply comply and remediate current systems minimizes front-end costs and organizational changes to, in the Gartner term, “map and wrap” existing processes into compliant systems. While it is easiest to observe this approach as it is applied to the standard transactions and code sets, it also is the approach being taken with privacy and security.⁵

Obviously, a decision to simply remediate existing processes does not lead to savings.⁶ It adds another translation step to current processes. Why is HIPAA viewed so narrowly and not as a major opportunity to improve administrative processes and achieve ROI?

One might start with a review of the missions and the challenges of healthcare organizations in 2002. Mission of course concerns providing patient care and the challenges are reducing medical errors, controlling costs, maintaining key staffing, and meeting patients/customers expectations. For example, if the Leapfrog Group’s analysis of the costs of medical errors (\$17 - \$29 billion per year with 44,000 to 98,000 avoidable deaths) are compared to the HIPAA estimate of a net \$19 billion in administrative cost savings over 10 years, what initiative would we expect a healthcare organization to set as its highest priority for investment? But it is HIPAA that has the highest priority because it is backed by government mandate.

Claims attachments

One of the areas of unfinished HIPAA business is the claims attachment standard. Claims attachments use ASC X12N transaction wrappers to convey HL7-based clinical data to support automated claims transactions. The initial six claims attachments have been ready for more than a year, but they have yet to be published even as proposed rules. While HIPAA rules have generally been late, we are unsure of when or, perhaps, if the draft claims rules will be put forth.

⁵ This approach has helped the Enterprise Application Integration (EAI) vendors to strong years. It also points to a fundamental approach to integrating new technology with legacy systems. We will see this with enterprise security and clinical information systems.

⁶ The Robert Wood Johnson Hospital reported on its cost-benefit analysis of using the standard transactions from its previous EDI/clearinghouse approach. Basically, new savings of approximately \$250,000 were balanced out by new costs of the same magnitude.

There is a growing concern within the standards community, specifically the Designated Standards Maintenance Organizations (DSMOs), that the time for claims attachment may be passing, and that there would be significant negative reaction to proposed rules now. We do not know the business case for automating claims attachment - how many claims have attachments. There is pushback from providers who see automation as an easy means for payors to delay payment with requests for additional data. Alternatively some payors are dropping routine use of attachments because they add work without increasing the likelihood of reduced payout. Finally, the current claims attachments are based on technology and four year old Health Level 7 standards. At one point, there was some consideration of using claims attachment as a means of introducing XML into the HIPAA process, but no work has really been done. In order to expect continued voluntary efforts to develop and maintain claims standards, HHS will have to decide what it is going to do. Given the basic decision not to reengineer processes to optimize the core transactions, claims begin to look like added overhead, not significant opportunity.

Privacy is doable.

While there are still significant outstanding privacy questions requiring clarification, most large organizations have done their assessments and are working on their policies and procedures. Smaller organizations have done less, but have less to do. Consents, authorizations, business associate agreements, and disclosure audits all add levels of administrative functions and documentation, some of which will be automated by HCIT vendors. "Minimum necessary" remains a murky area – again, more so for large and complex organizations and less so for smaller ones.⁷ Unless Draconian enforcement rules come out, most within the industry expect to at least meet the minimum privacy standards without running afoul of the "HIPAA police" by April 2003.

Security is the biggest issue.

The proposed HIPAA security rules came out in August of 1998. We still do not know when final rules will be published. We continue to hear that they will be coming out soon (by mid year?). One might legitimately question their value now. Although they might provide "safe harbor," they will not provide any greater insight as to how to secure a HCIT system. HCIT security has been defined by compliance with the proposed HIPAA rules for the last four years, not as a business priority. That changed post September 11th. It went from an IT issue to a CEO and board issue. In healthcare, security became much bigger and more important than securing protected health information. While the Security NPRM referenced contingency plans and back up, these jumped in importance along with emergency response and operational continuity in the face of disaster. HIPAA still looms as motivator, but more business attention is being directed at contingency plans, disaster recovery plus system protection, and not just maintaining privacy.⁸

⁷ "Minimum necessary" remains a HIPAA privacy requirement of great ambiguity. The clarification that a "care provider" can have access to the entire medical record for patient care purposes begs the issue of the role of the provider in the care process. First, of course, a care provider cannot have access to patients for whom they have no responsibility. Second, there remains a hierarchy of roles within the care team. Technicians may have no need to view nursing notes. There are areas of the medical record that are subject to higher levels of restriction than others. Thus, from a system standpoint, there must be policies and technical controls on who can access what for what purpose. The issue is the level of granularity of application function and data and whether authorization is based on real-time restrictions or later audit reviews.

⁸ The Porter report found that 92 percent of respondents identified HIPAA as the driver for security initiatives. However, 52 percent cited other, additional concerns.

Both the Phoenix and *CIO Insight* surveys have now caught up to this shift in their January surveys.⁹ Most healthcare organizations are really looking at threat analysis and risk assessments – but from a broader perspective than HIPAA. In their October survey, within a month of September 11, Phoenix found that only 8 percent of respondents indicated that their security plans would be impacted. Upon reflection, that figure has jumped to 65 percent in January.

The Porter report

At HIMSS conference, Cynthia Porter of Porter Research (www.porterresearch.com) presented a report on “Healthcare IT Data Security.” In the report, IDC data and their own research was cited confirming that security spending would increase 25 to 50 percent or more a year for the next several years. This would imply that security spending increases from 1.5 percent of total HCIT spending to about 3 percent over the next several years. This is a relatively large amount of “discretionary” IT spending. Security is clearly an IT infrastructure expenditure under the CIO. CIOs are relying on their primary HCIT vendors, who in turn were expected to partner with security vendors, such as Verisign or RSA. This is an example of the challenge facing HCIT – whether end-user policy or available technology should shape future products.

The business opportunity in Porter’s term is the lack of established brands in the security space. In our view, it reflects the failure of any vendor to come up with an end-to-end security framework for healthcare. Point products and technologies that address access control but not privilege management, or audit trails but not network security, are not the basis for ad hoc cobbling of diverse systems into a secure enterprise system. The absence of interoperability standards makes security integration that much more difficult.

Interoperable security systems - end-to-end

We cannot expect the HIPAA security rules to address the biggest technical issue – an end-to-end security framework that secures information at all points over its lifecycle. HHS must rely on existing ANSI standards for its rules. The SDOs and ad hoc initiatives have not developed such a framework. What we have are a series of “point” solutions with all else being “out of scope.” Security “points” include access controls (identification and authentication), authorization management, audit logs, data integrity maintenance and availability, and technical controls of the “network”.

Access controls

Access controls include user identification and authentication. We know this can be done with unique IDs and passwords, tokens, and biometrics. In general, policy says authentication should be stronger as physical controls and technical access becomes more remote. However, the same user might be local and remote to many systems. Single sign-on, while desirable from a user standpoint, introduces security risks and interoperability issues across system boundaries.

Authorization

Authorization (we know who you are but not what are you allowed to do) is a critical service in HCIT since there is a strict hierarchy of responsibilities for different caregivers. Physicians, nurses, therapists, technicians, and other aides, each have generic privileges that may be further restricted based on accreditations, local policy, and by patient identity. Within these authorization sets an individual may have multiple roles such as admitting, consulting, covering or attending physician. A secure system must enforce the granularity of technical restrictions based on identity and authorization rules, and/or support the same granularity in audit logs to capture inappropriate access or function. This is both a function of the privacy rules “minimum necessary,” as well as the absolute need for authority, such as writing a medication order or script. Authorizations, such as access control, are best viewed as a central service and function. However, most are now implemented by individual applications.

⁹ www.cioinsight.com - This is an all-industry survey. Look for the February 2002 issue.

Electronic Signature

Electronic and digital signatures occupy critical space in any security system. Currently, HCIT applications generally use a loose form of electronic signature as defined by JCAHO, which requires some unique user identification and an indication of signing. For example, a user logs on and adds a note. The action of saving the note might be described as an electronic signature of the logged on user. While this is acceptable at some practical level of clinical workflow, it becomes suspect in any rigorous challenge. For example, how strong is user identity enforced? Are passwords shared? Is there automated log-off? Moreover, once entered, how is the original data bound to the electronic signature? While there may be a set of policies, procedures, audits, and technical controls that in combination can insure authenticity and integrity, for the most part, we assume that very few electronically signed data will ever be challenged.

Digital signature, on the other hand, is a strong form that binds a certificate-based signature to the data and insures that the data cannot be changed without detection. Digital signature itself can be defeated by shared tokens (it is harder to spoof biometrics). Digital signature also requires a certificate authority (CA) to issue, maintain, and revoke certificates. The secure systems must be able to interoperate, sharing technical implementations and having common access to the CA. This "overhead" is public key infrastructure (PKI).

Digital signature can be used at the front-end as part of the identification step as well as for signing and data integrity functions. It can be used to encrypt data at rest and in transit. It can also be used as part of an authorization system if the certificate contains attributes that assign individual, role, or other authorizations. However, this greatly increases the costs and complexity of the CA authority and real-time certificate maintenance. Alternatively, there can be an enterprise network authorization service to manage authorizations, such as the OMG RAD. Least desirable is for each application to maintain its own user access and authorization lists.

Multi-SDO Digital Signature Project

In the Security NPRM, digital signature was identified as the only acceptable form of electronic signature for HIPAA purposes. For many technical and practical reasons, HHS has shelved the electronic signature rules at least until industry and the SDOs could come up with a new recommendation. In January 2001, a multi-SDO Digital Signature Project, chaired by HL7, was set up under ANSI-HISB to prepare recommendations to NCVHS and the Secretary. Two tracks were pursued. The first was to demonstrate interoperability among vendors in selected use cases, e.g., writing scripts. The second was to analyze the costs and benefits of a PKI in healthcare. Each in its own way has confirmed that digital signature rules are premature. The demonstration project has found little interest or support among vendors and federal PKI interest has waned. The Tunitas Group (www.tunitas.com) found at the outset of their cost benefit project that the legal basis of even digital signatures was still in doubt without pre-emptive legislation. Even PKI technology could be challenged if the rest of the system and supporting policies and practices could not be shown to be secure.

Audits

Audit trails work at a system, application, and data level. The Security NPRM is not clear on required usage. System level audits deal with log-ons, sessions, intrusions, and application server access. They do not deal with content or file access. Application audits are generally maintained by the applications themselves and record-user access to functions, patients, and files.

Audits and audit messaging are an area of current standards initiatives. The HL7 Security SIG has been meeting with the DICOM Security Workgroup, IHE, and NEMA to coordinate an audit message standard. Although there has been an action item for HL7 and ASTM to do a cross walk between the former's audit messages and the latter's audit content, that has not been done. The audit message standard would define the content of audit messages and common trigger events as well as transport formats. The content would be system-level events as discussed above. The evolving standard contemplates that such messages would be sent to an audit log repository. Actual use of the messages and logs are business policies and out of scope. In the US

representatives view, such audit messages, although not forensic in scope, could be part of a real-time alarm or alert system. According to European representatives, such use would be a violation of user privacy and the audit log would only be used retrospectively to investigate an alleged violation. We thus have a message standard (technology) developed independently of the business policies and rules.

The IHE, the ad hoc standards acceleration initiative jointly sponsored by RSNA and HIMSS (see www.rsna.org), has decided to move forward with an audit messaging function for its Year 4 demonstration, i.e., RSNA 2002/HIMSS 2003. While it is willing to use the HL7 standard if it is ready, the IHE will use its own "standard" in the likely event that HL7 will not have finalized and balloted its version until the fall as planned. The IHE and DICOM have already defined trigger events and data elements that could be implemented by imaging devices as well as participating application servers, primarily within radiology. If the IHE goes forward, we will then have a demonstration "standard", accepted within a limited domain, that will have to be aligned later with an enterprise "standard." While it is possible that HL7 and ASTM could conform their standards to the ad hoc standard, this is less likely given the broader constituency of users and applications. Moreover, while all parties want to insure that any audit standard meets all national requirements, in the United States at least, there is no input from the financial standards body, ASC X12N. Hopefully, there will not be multiple and competing HIPAA audit standards. This is a clear example of the problem of competing standards initiatives and the chaos they create.

Network controls and the need to remain technically neutral

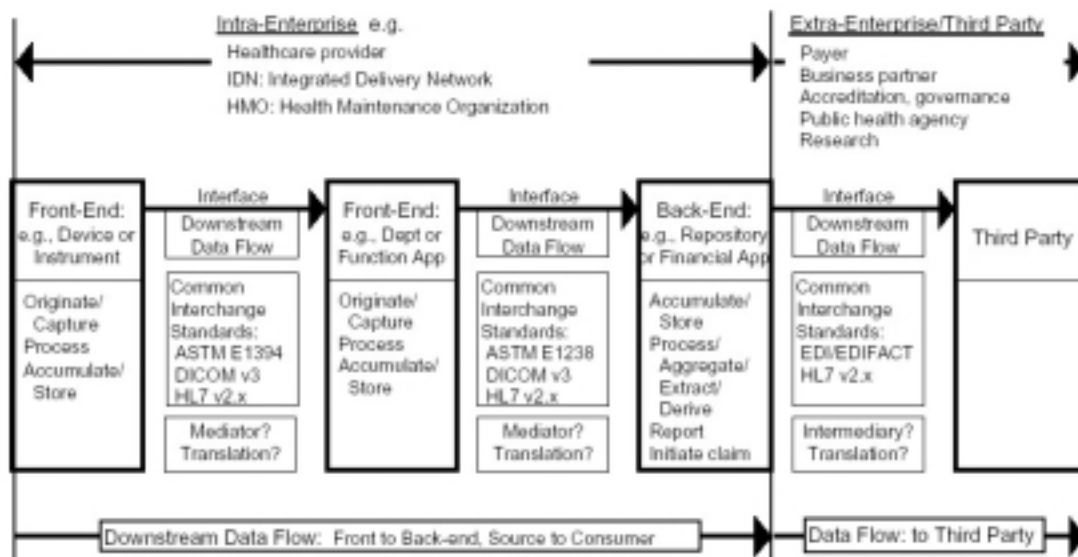
While we have traditionally thought of access, authentication, and insuring data integrity as user issues, they of course exist at the network, server, and increasingly at the medical device level. Network security within and without the enterprise is a far-ranging discussion beyond our present scope. Most HCIT systems have some form of authentication service provided by the network. Network transmissions include lower-level integrity services. Because HIPAA must be technically neutral, such controls are "handcrafted" based on the network operating system and configurations employed. In mixed operating systems environments and outside the firewall, technical and policy interoperability of all the security measures becomes much more problematic.

We should note another ad hoc security effort by the IHE. Since many of its members are imaging device vendors, it has an interest in securing these systems and their patient study output. DICOM is working on a digital certificate standard for devices, which will sign an imaging study prior to its manipulation and storage. More generally, IHE wants to address device-to-server and server-to-server security in their Year 4 demo. Making the assumption that individual devices and systems have adequate internal security, they seek to solve the problem of server-to-server authentication. Because of the devices, certain changes need to be made to standard server security mechanisms, such as SSL and single-key techniques. This again illustrates the strength and weakness of an ad hoc acceleration effort. They proactively solve problems quickly, but serially. It is left to determine if or how such an approach will work between a radiology system and the rest of the HCIT.

An E2E Security Framework

The problems faced in security are not individual technologies, but their integration within and between enterprise systems. Moreover, each security mechanism will impose overhead and costs on systems. How do all these point security solutions interoperate in concert within an organization outside the enterprise and over decades of time?

An approach proposed to the ISO Technical Committee 215/Working Group 2 by Per-Se is an end-to-end framework that identifies the roles and security responsibilities of the principal actors. The latter includes the data subject, creator, editor, translator, storer, user, and so forth. Conceptually, if each actor conforms to expected security norms, then all other actors can rely on the data without having to independently verify authenticity and integrity.



Partial diagram from: Healthcare Informatics Trusted End- to-End Information Flow
ISO TC 215/WG2 Working Draft

Technical Contact: Gary Dickinson (Gary.Dickinson@per-se.com)

Without such trusted end-to-end information flows over the life cycle of information, a significant amount of overhead must be expended to insure all data can be validated independently. Such a framework can provide organization for the roles of the point technologies. Moreover, it provides the system structure necessary to legally defend the medical data within, a weakness in even the strongest point security mechanisms.

We will watch the progress of this proposal and other security frameworks as matters of highest strategic importance.

HL7 Winter Working Group – January 2002

Overview

HL7 held its Winter Working Group meeting in early January in San Diego. Although no official attendance was announced, it appeared to be down 15 or 20 percent from the Fall Plenary and the year prior winter meeting. We speculate that this was primarily due to tightened travel budgets more than travel safety concerns. However, HL7 continued to draw strong representation from international and first-time attendees (both represented about 15 to 20 percent of total attendance). While this breaks a steady pattern of growing participation, HL7 still represents the primary source of clinical standards.

We have noted before that the strength and weakness of HL7 is its wide market acceptance and broad representation of diverse interests including active international affiliates. In the long run, this big tent will produce a strong, well-accepted standard. But in the short run, such multiplicity of competing interests slows progress compared to an initiative not as burdened with consensus methods and diverse stakeholders. In the world of XML, the Internet, and W3C, such deliberations invite ad hoc initiatives to create “point” solutions. For example, ASTM E31 Healthcare Informatics Committee is creating a series of XML DTDs for specific reports such as surgical and discharge. While these will serve specific purposes, particularly user readability and reduced XML overhead, their data content may not be easily mapped to other uses and system interoperability is not addressed. We have found as a general rule that one must deal with interoperability complexity either upfront in design or at the back-end in implementations. No

government mandate, standards acceleration initiative, or vendor product avoids the pain. It is simply a question of when it is faced and how much it costs. Rapid prototyping is useful in either approach, but until the devils in the detail are addressed, one is dealing with prototypes and demonstrations, not plug-and-play production systems.

HL7 leadership is attempting to balance and coordinate competing forces:

- The complexity of Version 3.0 against the time pressures to deliver
- Finishing Version 3.0 while maintaining Version 2.x
- Adapting Version 3.0 (machine optimized) messaging to Version 3.0 (human readable) clinical documents needs
- Supporting electronic health records (EHR) initiatives outside of the Clinical Document Architecture (CDA)
- Reference Information Model (RIM) -derived XML messages and documents versus simpler XML report standards
- Security needed from external standards
- RIM-based orders/results mapping to DICOM imaging and structured reports
- International interests, such as alternative billing systems, and US requirements, such as HIPAA claims attachments

For this report we will review Version 3 and the CDA and touch on security.

Version 3.0 Update

We have described previously that HL7 faces many challenges in producing its Version 3. The goal is to eliminate the ambiguities and variance found in the implementations of Version 2.x messages. To accomplish this, HL7 built a healthcare reference information model from which to derive messages and clinical documents. Understandably this is a major undertaking, complex in scope, methods and details. As we have found with HIPAA, constructing a specific implementation means many details have to be considered up front because the back-end flexibility is gone.

We noted that HL7 leadership has decided to push as much detail out of the RIM down into its various technical committees with domain responsibilities, e.g., medical records, observations, and results. The first ballot raised many objections, which HL7 is busily resolving. They have shifted from a problem in which the core modelers were getting too far into details to one of coordinating many TCs and keeping them within the bounds of the RIM and its methods.

At the core model, HL7 faces the issue of how to handle change. One would not want to change the RIM to accommodate every new or unanticipated data type and attribute. A change to the RIM, which impacts the entire messaging and CDA structures, should be rare. On the other hand, HL7 has already found many details that are not well accommodated by the RIM. For example, security and business rules are needed, but not present. In the model hierarchy, there is a cascade of added details and constraints as one moves from domain message information model, to RMIM, to the message definition, to the actually implemented message. Technical leadership must determine how, when, and where to handle extensions, variants, localizations, and optionalities. In general, HL7 expects that anyone proposing a variant must submit it to HL7 for formal inclusion in the standard. Internally, there is a problem reconciling the flexible, XML-based CDA to the more rigid (plug and play) model methodology.

The Clinical Document Architecture (CDA)

The CDA is a three-level clinical document specification using XML. Its historic roots were the KONA project and its first formal ANSI standard predated Version 3.0, although it was aligned to the then-current preliminary version. In reality, the CDA was checked for completeness against Version 2 messages. Level 1 fundamentally provides the document header and is human readable. Level 2 adds constraints (required structure or template) depending on document type, e.g., a prescription. Level 3 provides more detailed mark-up than Level 1, e.g. a medication must have certain attributes.

The tension between CDA and Version 3.0 is the desire to retain the “document” amidst messaging structures. Is the CDA optimized for machine processing or human readability? It is the data and container issue. Is CDA a set of schema for viewing a set of data from messages? That is not the same as saying this is the clinical document as it was created, edited, signed, and stored. The CDA is a context structure for content that is derived from the RIM. One might view Level 3 as one transform away from the human readable Level 1. Without new solutions, we are still at the issue of storing data and structure together as document as well as the data itself for application processing.

In evaluating the use of structured data within a structured document, one must deal with the clinical process issues of data granularity, electronic signature, and confidentiality. One has a choice of great detail in the header or scanning an entire document. Like HL7 in general, the CDA is just beginning to wrestle with security.

The CDA faces another challenge in trying to automate methods for deriving Level 2 and 3 documents from Version 3 methods. Since documents can combine multiple data types, the permutations of document DTD/schema can become much too large for handwiring. Bob Dolin, a co-chair of Structured Documents, is attempting to map RMIMs to the CDA body. For example, is a CDA body section an act in a RMIM? This mapping must be completed in order to develop automated tools between the messaging methods and the CDA. Since the messaging tools themselves are immature, this creates even greater difficulty for the CDA effort.

As we discussed above, there is a general desire among the Version 3 modelers to restrict changes, particularly as one moves up the hierarchy. This is in conflict with the use of local mark-up in the CDA. XML is inherently more flexible than a definitive model will allow.

Security in HL7

Security is generally viewed by HL7 as an out-of-scope service. That is not to say that the Security and Personnel SIGs are not concerned with security issues, including audit messaging, identity and authorization certificates, and digital signature as we have described above. However, technical leadership would rather wait for external standards from security experts than developing expertise and expending energy within HL7. The RIM does not model security actions for messages and clinical documents. Messages can be digitally signed and encrypted and one can create composite messages with different digital signatures. When the only role of HL7 was passing standard messages over the wire, this posture was understandable. Security, in all its aspects, was the province of the applications, servers, and network. Making the messages secure in transit was an external function. But that no longer is the scope of HL7 as it seeks to derive messages and documents from a reference-information model. Like the FedEx model, insuring secure delivery is one thing, insuring the authenticity and integrity of the payload is another.

This opens an opportunity for confusion or cooperation among various standards initiatives. We need to watch how security comes to HL7.

None of the foregoing should be viewed as a negative assessment of HL7. HL7 is challenged because it has chosen hard challenges. It has strong leadership, a driving vision, and wide support. The problems with which it is wrestling would have to be solved by any alternative standards initiative within the clinical domain. It is pay now or later.

Next Issue

We will update the status of the HIPAA standard transactions from the WEDI-SNIP perspective. We also will look at Web services, the W3C and ebXML as platforms for healthcare standards. Please direct any questions, suggestions or comments regarding *Standards Insight* to Joyce Sensmeier (jsensmeier@himss.org) or its author, Ed Larsen (erlarsen@erlinc.com).