



Standards Insight

An Analysis of Health Information Standards Development Initiatives

May 25, 2001

This information, prepared as a benefit to CHIM member firms, 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 CHIM's standards development analysis reporting efforts on your behalf are valued.
©Copyright CHIM, 2001. All rights reserved.

Contents

Introduction	Page 2
HIPAA is setting the agenda	Page 3
The New Standards – Regulatory Cycle	Page 4
Standards Development Organizations	Page 4
ASTM E31 Healthcare Informatics Committee	Page 4
HL7	Page 5
Digital Signature	Page 6
Government	Page 7
Users	Page 8
The HCIT Industry	Page 9
Conclusion	Page 9

Introduction

CHIM began the *Standards Insight* a year and a half ago to provide a business analysis of interoperability standards initiatives for its members. Interoperability standards create the strategic environment within which most HCIT vendors must develop and sell their products. Even the smallest healthcare organization will have more than one application and require some level of system integration. Interoperability is a condition for selling new applications. In the US, interoperability standards have been a voluntary effort, usually within the context of an ANSI accredited standards development organization (SDO). This has insured open participation and a consensus process among all interested parties. It also implies the need for SDOs to build market acceptance among users and vendors. We have noted in the past that HL7 and ASC X12N have been most successful in producing widely used standards in the clinical and financial realms respectively. HIPAA is changing the rules for developing interoperability standards. Not only do HIPAA's Administrative Simplification based regulations mandate specific standards for financial and managed care type transactions, but they have set up a framework for mandated interoperability standards in the future. This "shortcut" around voluntary market acceptance is increasingly being seen by many within the voluntary SDO community as their path to success. In turn this reduces the influence of end users and their vendors, the traditional source of SDO resources, as the standards industry becomes much more aligned with federal regulatory and financial services industry interests.

This shift has very important strategy implications for CHIM members, more so than specific the standards, so we will review the key standards initiatives within this context. Standards initiatives are going from enabling IT to setting IT agendas.

Be careful for what we ask for . . . we might get it.

HIPAA is setting the agenda

Despite or because of Secretary of HHS Thompson's decision to leave April 14, 2001, as the effective date for the privacy rules, there is an ongoing struggle to change and delay many of its provisions. HHS spokespeople have indicated that HHS will publish guidance to correct misinterpretations of the privacy rules in May and new proposed rules to fix recognized errors, such as "prior consent" rules and use of J codes, over the next year. In fact, the administration will probably make significant change to the privacy rules even though the two-year clock is running.

No responsible party to the debate is against protecting the privacy of an individual's health information. Yet the AHA, AMA, Blue Cross/Blue Shield and other health insurers, pharmacists and others oppose the specific privacy rules published. HIPAA was sold as an industry requested mandate to accelerate standards in order to save significant money wasted in financial and managed care transactions. What has been delivered is an intrusive, far-reaching mandate covering all forms of PHI requiring significant new investment by the covered parties. Although one expects "covered parties" never to welcome regulation, the negative reaction to rules purported to save \$12 billion is very pronounced. There are real consequences to the privacy and related security regulations – they change spending priorities.

HHS has estimated that all covered will spend \$17.6 billion to implement the privacy rules in addition to the \$7 billion for implementing the standard transactions. Through slight of hand, HHS avoids estimating the costs of its yet to be finalized security regulations. Instead it says that these are a cost of doing business and were included in the cost benefit analysis presented in the final transaction and code rules.¹ Nonetheless, it is not difficult to see how the AHA might estimate that it would cost its hospitals \$22 billion to comply. Not only is this an unfunded mandate but it will displace other spending. Recall that the AHA estimated that its members spent \$8 billion for Y2K. Recall also how this spending effectively stopped spending on new IT initiatives. Despite improving operating margins following the BBA givebacks, capital availability is one of the highest concerns of hospital leadership. The total operating profits of all hospitals is now about \$10 – 12 billion a year. In this year's HIMSS Leadership Survey, not surprisingly, HIPAA was the highest priority of healthcare organizations. This represents setting real priorities. It displaces other IT related initiatives, such as medical error prevention.

Thus through regulations, HHS is directing the healthcare industry to spend money on patient health information privacy and security in preference to medical error initiatives. It is not at all clear that HIPAA will accelerate anything but it is likely to be expensive.²

¹ The cost benefit analysis of the security rules components of Administrative Simplification only included the costs of securing the specific transactions, not all forms of electronic data stored and used by covered parties. It is this latter overreach of the federal regulators that has caused the industry reaction.

² Most industry reports indicate that hospitals have not spent significant amounts yet on HIPAA and more importantly have not put much into their next year budget. This leads some observers to the belief that HIPAA will be delayed and modified because no one will be able to comply. This, in turn, leads to an interesting form of "civil disobedience" to thwart poor rules. We will see how things proceed when the enforcement rules are issued late this year.

There is a further perversion in federal regulations, particularly in the area of technology. They lock in the technical solution set to that available and in an existing ANSI standard at time the rules were enacted. An example of this is XML. Not an approved standard at the time the transaction rules were written, XML is written out of use in the covered transactions until such time as standards are developed and incorporated in changes to the federal rules. Who will be willing to demonstrate the use of XML, which now is explicitly not permitted by law? The security rules will similarly freeze innovation and/or force marketing efforts to be directed at selling the regulators and their SDO proxies, not customers. Smart SDOs are turning their focus to the next things that the federal government will mandate, such as digital signatures and the electronic health record data elements.

The New Standards – Regulatory Cycle

As healthcare information systems become a more regulated industry, we can outline the cycle that SDO's and savvy HCIT vendors will follow to win in the market.

Standards Development Organizations

Under the HIPAA model, HHS is required to adopt existing ANSI standards, when they exist and with the advice of the National Committee on Vital and Health Statistics (NCVHS). Unless Congress or the current administration limits the scope of HIPAA, HHS is authorized to "improve the efficiency and effectiveness of the health care system by encouraging the development of a health information system through the establishment of standards and requirements to enable the electronic exchange of certain health information".

Thus the first player in the game is an ANSI accredited SDO, e.g., ASTM, ASC X12 or HL7 but not DICOM, WEDI or ebXML, etc.) The SDOs need to identify and define key turf to establish their franchise. ASC X12 has done so in the financial/insurance arena, ASTM E31 in privacy and security and HL7 in clinical messaging. The problem is when there are conflicting turf claims. E31 has established standards for the data elements for an electronic health record while HL7, de facto, creates a competing standard through its RIM and eventually level three of its clinical document architecture. How can clinical data element standards not interact with clinical message content standards and vice versa? In prior times we would expect the market to decide if and which standard to use. However, with the new HIPAA model in place both will compete before NCVHS and HHS to be selected as the basis for EHR data element rules. In fact E31 along with the American Health Information Management Association (AHIMA) is conducting a survey of users and vendors to determine familiarity with the existing ASTM E 1384 Standard Guide for Content and Structure of the Electronic Health Record. Since it is unlikely that many in either industry or the end user community are familiar with the standard, the survey goes on to ask the respondent to verify that the data elements included in E 1384 would be used in an electronic health record. Since most of these data elements are obviously common to any EHR implementation, e.g., patient name and DOB, the survey will validate that many of the data elements in E 1384 are used even though the standard itself is unrecognized. Thus one might claim that E 1384 is widely implemented – a plus before NCVHS – say in contrast to a record derived from HL7's RIM.

The dynamics of the SDO world are subtly changing from consensus advancement of the interests of their members' sponsors to supporting federal regulators agenda.

ASTM E31 Healthcare Informatics Committee

The Executive Committee decided to trim and focus the E31 Committee. Specifically they will organize their sub-committees around two areas: privacy and security and the electronic health record. Other subcommittees, such as those dealing with laboratory information, controlled vocabulary and modeling will probably be spun off to other SDOs. This is the clearest recognition of how the SDOs are reacting to the changing environment.

E31's major privacy and security initiatives include developing a standard for PKI, for privilege management infrastructure and directory services. These services underlie the security framework. The framework establishes the technical basis of access control, authentication, authorization and data integrity. This goes far beyond single log-on and establishing roles. For example, if certificates are used, do they contain authorization information or only authentication data? The answer to that question ripples through the technology and policy of a whole system. The E31.20 security subcommittee also is evaluating a proposal to sponsor the Object Management Group's resource access decision facility specification as an ANSI standard. While there are copyright and control problems that will probably preclude this, the subcommittee was impressed with the technical service and might elect to produce an implementation guideline, i.e., standard, for implementing RAD. RAD or a RAD like service will be necessary for managing fine grain access to patient information among multiple applications. While log-on access control and role based authorization can establish who and what someone is, there is a next level of dynamic control needed to match providers with patients and application functions. It would be an administrative nightmare if each application had to manage such access.

E31's second focus is the electronic health record. It has already published E 1384 as discussed above. In addition, E31 is working on standards for XML based documents and the personal health record.

HL7

HL7 has been relatively slow to get into the federal regulation game. We discussed in an earlier issue their inclusion as a Designated Standards Maintenance Organization by virtue of the use of HL7 messages in the yet to be published HIPAA claims attachment rules. However, as also discussed in earlier issues, they were late to the security game, only recently including certificates (credential attributes) and signature concepts into the RIM. (See next discussion on digital signature.) In the old world of voluntary standards organizations, HL7 was the market brand leader. In the new regulatory environment, it is losing its influence. First, the financial-administrative side of the industry, the WEDI-led group, is setting priorities, engaging the covered parties and making decisions to enable the financial transactions and codes. Second, HL7 is itself struggling to move Version 3 forward. Version 3 is based on a healthcare information model, a very major and complex undertaking. It has embraced forward-looking technology, such as XML and automated tools. In some cases these technologies move faster than can the healthcare content. All of this is done without a clear market mandate. Thus the HL7 leadership must evaluate if they should move closer to the regulatory realm, e.g., NCVHS, cut back the complexity of Version 3 to get it out or fight the old fashioned way to lead users and vendors to demand HL7 compatibility.

HL7 takes considerable pride in its decision to aggressively pursue international participation even though it is an American National Standards accredited SDO. On balance this appears to have been a big plus. While international needs and interests often slow down the consensus process, their different perspectives provide the diversity of positions needed to develop robust standards. Right now, this broad perspective may limit, HL7 in responding to US political issues.

Ultimately HL7 will win out because its standards deal with clinical data, the source data of healthcare, and are in wide use. One cannot make patient information more accurate, authentic, secure or private after it has been created. These are not add-on functions. The danger is that before the regulators, security experts and other SDOs figure this out, there will be a layer of poorly crafted clinical standards in place. Digital signature may be the first opportunity for such mischief.

Digital Signature

The original NPRM for security also included rules for electronic signatures. In essence the latter said that if an electronic signature was used in a covered transaction, it must conform to certain standards. At the time, only digital signature met those standards. Subsequently HHS is reported to have backed off on the proposed electronic signature rules, primarily due to a concern that the technology was not ripe for regulation.³

As we recounted in the January 22, 2001 issue of *Standards Insight*, HL7 discovered its need for including signatures and authorizations in its RIM and clinical document architecture. Concurrently the WEDI and NCVHS recognized the need for electronic signatures in upcoming attachments. The PKI community also wanted to get HHS to move forward on electronic signature standards. Because ASTM E31 had published standards in this area (their turf), a multi-SDO meeting was held at the HL7 meeting in January. This group was subsequently blessed by NCHVS and embraced by ANSI HISB with the charter to produce an electronic signature standard, presumably based on existing standards and demonstrated use.

³ Some notes of clarification. Electronic signature and digital signature are not synonymous. The former is any electronic form meant to convey the traditional meaning of a signature, an intent to sign. These include keystroke series, facsimile, scanned, id-password pair or digitizing tablet. Each of these methods has value but also drawbacks when compared to manually signed documents. These include ease of forgery (allowing repudiation) and binding of the signature to the data/document signed. A digital signature can be used as a form of electronic signature and as such adds much more strength. When properly protected in hardware, a private key can lock and encrypt both the signature and the data signed in a manner in which it can be viewed but never changed – at least without easily observed evidence of such change. Digital signature requires a fair amount of overhead (e.g., smart cards) and infrastructure, e.g., public key infrastructure (PKI) to work properly. Digital signature technology is also a means of insuring data integrity. The HIPAA security NPRM notes this within the context of security, which raises a worrisome nexus between use of digital signature technology for transactions and more broadly within security framework.

The clear endpoint of this effort will be a HIPAA derived standard for electronic signature in healthcare. The question is whether such standard will only apply to HIPAA transactions, or to use within a HIPAA compliant security framework or anywhere in healthcare. The group has explicitly said it will not limit itself to the first application – use in transactions – and for good reason. However, this is exactly the same line of reasoning that led to HIPAA administrative simplification being extended to mandate privacy and security rules for personnel health information. The reason one cannot easily restrict the standard to transactions is that the FedEx function, insuring the integrity of a message from sender to receiver, is a modest part of the problem. The real issue is the integrity of the content, e.g., is this consent actually signed by a patient, is this physician note really what the physician wrote at the time specified, does the nursing assessment really reflect the state of the patient at this point in time. In today's environment medical records departments will send copies of the provider's medical records as they are created and maintained in the normal course of business. These are substantially paper documents with handwritten initials or signatures, perhaps rubber stamps. To move this to the "electronic health record", one must have the analog of these handwritten signatures. Moreover, one must put processes and restrictions into place that insures integrity of the electronic form. Today the good and bad feature of a paper chart is that it can only be in one place at a time – frustrating when it is not where you want it but much easier to physically secure than is an electronic record.

The Multi-SDO Digital Signature Project (as it is formally called) already shows the bias problem. Digital signature as a technology may not be cost-effective or even technically feasible as a replacement for a manual signature in all healthcare applications and documents. Yet if ultimately one expects a chain of trust from nurse input to final medical record, from physician order through medication delivery, from patient consent to malpractice law suit, a chain of trust defined by digital signature, then all the links must meet that standard. You cannot apply authenticity and integrity later. Conversely, if all electronic records are bits and pieces of diverse signature technologies what can one say of the composite record?

These are valid questions, much more so within the context of mandated standards for data elements within an electronic health record. It will be important to apportion the cost and value between improving patient care and requirements to respond to legal actions.

Government

The history of HIPAA Administrative Simplification from its early 1990's days to its present form would be an interesting story to retrace. In the previous *Standards Insight* (March 19, 2001), we discussed the expansion of privacy and security beyond protecting the mandated transactions to all private health information ever touched by a covered party. We also noted the open-ended mandate for HHS to mandate adoption of data standards for patient medical record information. While few would argue against a public policy of insuring the privacy and security of personal health, there is debate about the priority among all of the things for which healthcare organizations could use free cash flow.

This readiness to reprioritize spending by the healthcare industry is made more questionable by the inexperience with the methods being applied to a very large and complex service segment of the economy. HHS readily admits that it does not know what the impact of HIPAA will be. Few industries, outside the national security arena, have systematically implemented standard privacy and security rules with so little time or proven experience⁴. While it is easy to indicate that each covered party, whether solo practice or large insurer, must do a risk assessment and then adopt reasonable policy and procedures, we have no guide to reasonableness or how to scale this for size and location. This is without considering the incremental requirements and liabilities of state laws.

HIPAA administrative simplification rules have been sold as good enough to make a beginning. The intent is to be reasonable and fix things as we go along. The reality is that there are now federal rules in place where there were none before setting the priorities, processes and methods to be used by insuring PHI privacy and security. We will know more about reasonableness when HHS publishes the enforcement rules later this year.

Users

There are at least three distinct vested interests among the end-users. For traditional providers and health plans, or covered parties in HIPAA terms, there is the prospect of less expensive “managed care” transactions. As we noted in the previous *Standards Insight* it is unlikely that the covered parties will reap profit from this investment as outlined by HHS since the ultimate payers, such as Medicare and employers, will extract such profit by negotiating their payment rates downward. Thus this is really a cost of doing business that everyone must incur. Moreover, there are the incremental costs of implementing the privacy and security rules, another added cost of doing business. The AHA is seeking reimbursement for these expenditures, an otherwise unfunded mandate that comes out of the hide of operations and hence improvements in patient care.

These are the bricks, which will absorb the most costs because they have legacy systems and established workflow processes. The clicks, the new e-health industry, have a different agenda. They begin in many respects with a new business model and less legacy to remediate. Moreover, as they seek to engage the consumer, making healthcare a real service industry, they need to have a “trust wrapper” insuring personal privacy. In fact if it were not for the new virtual healthcare enterprises and explosion in electronic information there would not be the high level of public anxiety about privacy. Thus to solve the clicks needs, the bricks will pay.

Behind the scenes the public health and medical researchers and data miners are anxious to get their hands on increasingly richer and more available computerized data. They too have an agenda and need. For example the Agency for Healthcare Research and Quality (AHRQ) representatives believe that patients will not provide data to their physicians and hospitals if they are not assured of its privacy. If patients do not provide the information, then it will not be available to researchers. While there may be some truth to this proposition, the solution way overshoots the mark and once again the bricks pay so the government and pharmaceutical researchers can get de-identified data. In fact, HIPAA privacy does not allow the individual to opt out of use of their de-identified data.

⁴ Of course the financial services industry is working its way through the Graham-Leach-Bliley rules and has had to develop extensive security rules to protect financial assets. It is doubtful that security experiences in the financial services industry will readily transport to providing patient care. Unfortunately, Administrative Simplification is the financial tail wagging the clinical dog.

The HCIT Industry

As HCIT vendors and consultants, we face a mixed bag. In the next few years, HIPAA consulting, re-architecting and remediating current systems will mean big dollars for some in our industry. HIPAA driven spending will be at least similar in magnitude to that preceding January 1, 2000. Conversely, it is likely that new IT initiatives, such as clinical systems, physician order entry and electronic health records, will be deferred. Internal client resources and funding will not support both HIPAA mandates and new initiatives. While some CIS vendors make the case that automating clinical documentation and processes is easier than securing a paper based system, it is unlikely that executive management will make such a leap of faith.

An interesting phenomenon is that HCIT industry has generally taken a political stance opposed to that of our ultimate customers, the healthcare organizations. While some within the industry will reap significant HIPAA revenue, we will do so against the expressed interests of our customers. We might want to consider publicly promoting our self-interest over that of our customers. Moreover, we, better than most, know what will not be done because of the spending on HIPAA privacy and security.

Conclusion

HIPAA is having a corrupting impact on standards development in the US. A pattern for power has emerged by getting the federal government to adopt standards from one's organization and make them mandatory. It creates sustainable organizational power and individual opportunity unlike any that are conferred by ANSI. For better or worse HCIT vendors and consultants need to note and act on this change in the environment if they are to be players in defining the future of HCIT.

Publication of the *Standards Insight* will be suspended after this issue while CHIM and HIMSS determine whether to reunite. In either case, there will be a re-examination of all member services. If you have found *Standards Insight* to be useful to your organization please provide this feedback to [Carla Smith](#) or its author, [Ed Larsen](#).