



Standards Insight

An Analysis of Health Information Standards Development Initiatives

August 27, 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 and Overview	1
HIPAA	2
Privacy Rules	2
Security Rules	3
Standards for Patient Medical Record Information	4
PMRI Strategy	6
Voluntary versus Regulated – An Alternative View	7
Next Issue	7

Introduction and Overview

The *Standards Insight* is intended to provide business strategy analysis of key standards initiatives, an important facet of our shared market environment. This issue will again start with an update on HIPAA imposed standards, particularly those from the Privacy rule. However, HIPAA Administrative Simplification is rapidly moving from being a strategic issue to one of tactics and implementation. Thus we will provide an overview of the next HIPAA, standards for Patient Medical Record Information. It serves as a framework to briefly review clinical interoperability standards initiatives. It also is at a point of strategic interest to the industry – a point to begin considering opportunities and competitive positioning.

HIPAA

HIPAA Administrative Simplification¹ occupies a central focus of interoperability standards initiatives and indeed of healthcare information technology. While we are all quick to point out that much of HIPAA compliance requires our customers to develop policies and procedures and to implement sound business practices rather than investing in computer systems, HIPAA is having a significant impact on the healthcare information technology industry. It is in two forms: the opportunity and the opportunity costs. The mandated standard electronic transactions require new software and workflow implementation. Privacy rules require policies and then systems to manage consents, authorizations, revocations, disclosures, and requests for limitations involving protected health information (PHI). Privacy also requires both policies and systems to insure that only the minimum necessary PHI is used internally and disclosed externally. The yet to be finalized Security rules will require specific technical mechanisms and safeguards to protect privacy, insure availability and maintain the integrity of PHI. All of these requirements will consume a significant amount of human and financial resources in a marginally profitable industry. Whether or not HIPAA exceeds the costs of Y2K is beside the point. It is certainly enough to divert funds and disrupt other HCIT initiatives. If the HHS estimates are in the right ballpark, then HIPAA will cost hospitals and other covered entities almost what Y2K did.² This represents great opportunity for some, such as consultants. Others, particularly large core system vendors, will use HIPAA to gain competitive advantage. However, HIPAA compliance will divert key personnel and funding away from other large HCIT initiatives, such as reducing medical errors or automating clinical workflow. Some of our customers, the most adroit, will find solutions to HIPAA through automation of clinical process and the EMR, but it will be few covered entities that can fund and tackle such large projects in timely manner. For most covered entities, serial problem solving and limited resources will necessitate HIPAA compliance as the next big thing, displacing other discretionary projects.

HIPAA has moved from the realm of strategy to that of implementation. The Standard Transactions and Codes have received the most effort so far. The WEDI Strategic National Implementation Process (SNIP) is coordinating multiple test implementations. Many of the recent recommendations³ from the NCVHS to HHS for necessary revisions, such as continuing to use "J codes" for drugs in hospitals, reflected the problems found by SNIP. There are strong reasons to believe that all plans and providers will not be able to meet the October 2002 compliance date. A 12 to 24 month delay is a likely compromise. However there is general agreement that the Standard Transactions rules should go forward.

Privacy Rules

Such consensus is not the same case for the Privacy rules. Few would publicly attack the politically powerful promise of insuring the privacy of personal health information. However, as the covered entities really begin to evaluate policy and procedures, the result of HHS' decision not to change the effective date⁴, they are finding many problems and unintended consequences.

¹ We will continue to use the term HIPAA to mean its Administrative Simplification provisions including Standard Transactions, Privacy, Security and so forth.

² HHS estimated the cost of complying with the transactions and privacy rules to be \$17.6 billion over 10 years. Much of the costs are front loaded and do not include the incremental costs of extending security beyond the covered transactions to all PHI in computers, on paper or orally communicated. The AHA reported that hospitals spent \$8 billion on Y2K remediation. If hospitals incurred a quarter of the estimated costs, if the costs of security are added in and most of the total are incurred in the first few years, it gets one close to \$5 or \$6 billion. It is unlikely that the government has overestimated the costs. The AHA has advanced costs estimates of over \$20 billion.

³ NCVHS Fourth Annual Report to Congress on the Implementation of the Administrative Simplification Provisions of HIPAA (sic), March 22, 2001. See www.ncvhs.gov.

⁴ This is the good and bad news of accelerating standards. By forcing users to begin implementation because of hard dates, you begin the experiment and start finding the problems.

In July, HHS⁵ issued its first set of guidance, highlighting key areas of the rules that it intended to clarify or fix.⁵ Consent and minimum necessary are two primary issues that impact HCIT.

The just completed NCVHS Subcommittee on Privacy and Confidentiality hearings sought to better define these issues and develop further recommendations for HHS.⁶ It is clear that the Privacy rules themselves are complex with competing requirements. For example, the minimum necessary rule does not apply to required data in a covered transaction, but it does apply to optional fields in the transaction. Minimum necessary does not apply to information requests necessary for treatment between covered parties but a covered party must adopt a minimum necessary policy for internal use of the data. While such policy might say any caregiver assigned to the patient should have full access to all patient data, this immediately breaks down in the complex reality of multi-disciplined teams, temporary staffing and the multiple uses to which data is put. If this is confusing how does one write the access control and audit system requirements for insuring minimum necessary use of PHI?

There is also mounting concern surfaced at the subcommittee hearings that the covered entities are adopting highly defensive and restrictive approaches for the use and disclosure of PHI. Each is seeking to remove itself from the perceived legal liabilities created by the rules themselves and from the expected lawsuits.⁷ This trend may significantly impede the flow of patient data, the opposite of Institute of Medicine recommendations for reshaping health care.

As a final note on Privacy, several groups, such as the Association of American Physicians and Surgeons, have filed lawsuits seeking to block implementation of the Privacy rules. Grounds include violation of the bill of rights and laws governing paper work reduction and regulatory authority limitations. Success in any of these suits would further delay and confuse Privacy implementation. While we have no basis for judging the merit of such suits, we can note that there are many special interest groups that believe the Privacy rules in fact give too much sanctioned access to PHI by law enforcement, public health and researchers. Perversely, in mandating consents and disclosure of the policies for use and disclosure of PHI and seeking special authorizations, the Privacy rules might further induce patients to withhold information.

Security Rules

We will defer discussion of the still to be finalized Security rules as well as digital signatures for the next issue. We might note in passing that computer and network security is a rapidly changing environment. Security rules for healthcare information systems cannot be crafted solely within the context of our vertical industry. While internal breaches remain the most significant threat to PHI confidentiality, availability and integrity, the technical challenges are shared broadly across all industries. A red cross does not stop Code Red. Recent experience suggests that organizing information security by vertical industry loosely coordinated by the National Infrastructure Protection Center is not working when security threats can easily target any industry. Thus HIPAA Security rules must deal not only with the complexity of healthcare information and the HHS iatrogenic expansion of scope to include written and oral communication, they must consider a much broader information security framework.

The burden of good design and requirements definition is shifted from the front-end (a cost to the government) to the back-end (a cost to the user).

⁵ Available at www.hhs.gov/ocr/hipaa/

⁶ The subcommittee also considered marketing and research issues. See www.ncvhs.gov for transcripts.

⁷ HIPAA does not permit an individual to sue in federal court for violations of the privacy and security rules. However, it does not prevent such suits in state courts. The fear is that the HIPAA rules will be used as evidence of expected good practice or community standards.

Standards for Patient Medical Record Information

The National Center for Vital and Health Statistics is a public advisory board to the Secretary of HHS. Under HIPAA, the NCVHS has a broad mandate to advise the Secretary on ways to improve the efficiency and effectiveness of the healthcare system primarily through establishment of information standards. Specifically it was charged with reporting to the Secretary on standards for interoperable Patient Medical Records, i.e., the electronic medical record.

As a first step, NCVHS issued a preliminary report and set of recommendations in July 2000.⁸ In reality, the committee set forth some guiding principles and directions but, bottom line, deferred specific recommendations on standards pending more data and analysis. The committee set a timetable to make recommendations to the Secretary by February 2002. This month the Subcommittee on Standards and Security held hearings with testimony from the relevant Standard Development Organizations (SDOs). In October it will hold additional hearings for vendors and end users, including government providers.⁹

This month's hearing provides a framework for briefly updating the state of clinical interoperability standards. First, let us put the NCVHS initiative into some perspective. There is a general perception among some in HHS, NCVHS and the SDOs, the emerging "standards-industrial complex", that the HIPAA model for managed care standard transactions represents a significant and successful break-through in healthcare informatics. The Congress and HHS responded to the pleas from the payor and provider industries to mandate standards, which the industry was unable to impose on itself despite the claim of immense financial savings. The *Standards Insight* and others have examined these premises in many other forums and we will not repeat these here.

However, the "lesson learned" is that with government coordination and regulation, we can improve and speed the results of voluntary standards initiatives. NCVHS is generally applying this lesson to the EMR and clinical systems. The voluntary SDOs do not have the resources to produce widely used standards in a timely fashion nor are they able to coordinate their activities in areas of overlap. Voluntary, uncoordinated standards initiatives are no way to develop an information infrastructure for 14 percent of the GDP.

The stated goal of PMRI standards is to enable the exchange of comparable, quality patient medical record data between systems. One should note that there are many parties interested in such standards. Some benefits accrue directly to the patient; the potential for coordinating care among one's different care providers, the potential to move one's PMR between providers and the potential of access anywhere in an emergency. There are some benefits to care providers if they can integrate clinical information systems with minimal interfacing costs. But the largest benefits probably occur in the fields of cross-patient analysis, clinical trials, outcomes research and public health. The costs and complexity of obtaining clinical data are greatly reduced if all systems could provide standardized data. Of course these public benefits do return to the individual in terms of better care decisions, protocols and guidelines, evidence based medicine and improved outcomes. The trick is to figure out how to make the benefits to the data originators, the healthcare providers, sufficient to justify the system costs of implementing the mandated standard PMR.

⁸ Report to the Secretary of HHS Uniform Data Standards for Patient Medical Record Information. Available at www.ncvhs.gov.

⁹ The Subcommittee on Standards and Security is looking for input from vendors and end users on existing clinical messaging standards prior to and for their October 9-10 hearings. It has initially evaluated standards from HL7, DICOM, IEEE and OMG based on data supplied by the SDOs. The subcommittee now needs more input from vendors and end users to evaluate how widely accepted, costly and useful the standards really are. Vendors and providers will be invited to submit written testimony concerning specific standards and some will be asked to testify and discuss these at the October meeting. Jeff Blair (jeffblair@medrecinst.com) and Simon Cohn (simon.cohn@kp.org) are the co-chairs and points of contact.

A standards based PMR requires interoperability, which in turn requires message standards for content and context. Moreover, comparability and quality of data, a goal of public health and other data miners, are determined not just by technical system interfaces but by the performance of the clinician that originates the data. We are on a very slippery slope.

The subcommittee commissioned a survey of the SDOs to determine the capability of current clinical messaging standards to meet these requirements. Based on their initial recommendations with some modifications, they attempted to evaluate standards according to the following criteria:

- Market acceptance
- Interoperability
- Comparability
- Data quality

The analysis resulted in preliminary findings and ratings. First a number of SDOs were not considered since they did not produce messaging standards. For example, the ASTM E31 Committee E1384 standard guide for the content and structure of an EMR was not considered since it targets data at rest not in transit, i.e., messaging - a distinction that justifies interface engines more than interoperability. Similarly SNOMED and CPT terminology codes were not evaluated. Both address content and in some cases context so the position is arguable given that context and context must underlie any message.

On the other hand, HL7 Version 3.0, the only comprehensive messaging standard based on a reference information model (defining content and context including incorporation by reference external code standards) was excluded because it is not yet an ANSI standard and, unfinished, has no market acceptance. This points to a major limitation of HIPAA process based standards. In 2001, we are probably one year away from an ANSI approved Version 3.0. The analysis targeted Version 2.4, which is an ANSI standard but which has not yet widely displaced Versions 2.2 or 2.3, which are 5 years old. Would it make sense to develop PMRI standards based on widely used standards today, on the most current approved versions just being adopted or on next generation versions that will be available when implementation occurs? The federal rule making process freezes technology for at least five years, the time period from analysis and proposed rules until end users are implementing.

Based on submittals and the preliminary screening above, the following standards were rated: HL7 Version 2.4, DICOM, Open Management Group's Person Identifier, Lexicon and Clinical Observation services and the IEEE device interface. Although results have not been publicly posted, they were reported orally at the hearings. DICOM had the highest score, partly based on high market acceptance (self-reported). Without reviewing the data I am at a loss as to what this evaluation means. It could not mean that one is trying to decide whether HL7 or DICOM has a better standard for the PMR. Would one build a PMR starting with an imaging standard?

DICOM is widely accepted within imaging where it automates interfaces to imaging devices, storage and workflow systems. IEEE has a similar type role with medical devices but is not implemented widely. OMG is not an ANSI accredited standards body. Its services are very elegant and fill needs not well addressed by HL7. They have been used in the government electronic record project. OMG also has an potentially important security service, its resource access decision (RAD), that provides a finer level of access control than that provided at network levels. Among the submittals, indeed among US standards, only HL7 has the market acceptance and domain coverage to be considered as a basis for a national PMRI standard. However, Version 2.X offers too much optionality to make HIPAA-like implementation guides feasible. That of course is the point of Version 3.0.

No amount of evaluation and testimony is likely to obscure HL7's pre-eminent role.¹⁰ The RIM is a comprehensive and extensible model of healthcare information. In fact that appears to be its weakness – a perception by some within the standards-industrial complex that HL7 is too Microsoft-like. It embraces other standards and extends its turf. It has an independent agenda and its own constituency and is not dependent on government mandate for its success. On the other hand, ASTM E31 is planning to consolidate around fewer standards. DICOM is struggling between throwing in with HL7 or trying to develop competing structured report standards. Meanwhile IHE, the joint effort between RSNA and HIMSS that seeks to use DICOM to accelerate integration of the healthcare enterprise is still stuck in the workflow of imaging departments. OMG, like the Andover Working Group and Microsoft Active X for Healthcare before it, cannot overcome a technology and vendor bias to become widely accepted.

That said, HL7 is not widely used outside of acute care settings. As noted in the hearings most healthcare informatics standards are hospital centric. Most healthcare encounters, to be captured in a PMR, will not occur in the inpatient setting.

Finally as noted at the onset, in order for clinical data to be exchanged and be meaningful to other users, the data must be of standard quality and comparable meaning. This is not a messaging problem. It is a user problem. Users must agree on terminology and usage, agree to structure, to required fields, to coded value choices. We are currently seeing how hard this is to automate "simple" billing records based on UB92 and HCFA 1500 forms used for years. Automating the medical record is orders of magnitude more complex.

PMRI Strategy

There are three strategic paths for HHS to pursue. The first is for the government to do take a hands-off approach and let the market develop the EMR. The second is to provide coordination of voluntary efforts. Since the ANSI HISB is already in this role, the government would have to inject more funds and thereby exert directive control to consolidate the best standards. The third is to take over full direction and mandate standards. This is akin to the HIPAA approach. I would suspect that the lessons learned from HIPAA and the emergent standards-industrial complex will find the third option irresistible.

What we do not know is how HIPAA will really play out. The late Herb Stein, a leading economist, is quoted as saying "If something is unsustainable, it tends to stop".¹¹ There may not be enough funding and expertise available to HHS for it to figure out how to make privacy and security rules work, let alone an EMR. Although the Bush Administration elected not to challenge the politically popular concept of patient privacy protection, there is evidence that it does not want to impose more regulation on the healthcare industry. The problem is that the situation is unstable. Either HHS gets further into creating detailed safe harbor policies or it must signal a very liberal interpretation and lenient enforcement approach to Privacy and Security.

The standard PMR will not happen in the next several years. Developers cannot begin to use it as a template for product design. With more immediate business concerns, why spend time on the PMR now? Because now is a time for the HCIT industry to evaluate these issues of voluntary or mandated standards and to help shape direction. Certainly individual industry companies will want to decide if they are leading players, or seeking competitive advantage or willing to accept what comes along.

¹⁰ It should be noted that HL7 is an American National Standards approved SDO with international affiliates. However, it is not an international standards body in the sense of ISO, nor is it a European Union or other national standards body. There are at least two other EMR standards in the world marketplace that are as comprehensive as HL7 Version 3. These are from CEN and the Australian GEHR.

¹¹ The quotation was used by Thomas Maeder in the September 1, 2001 issue of *Red Herring*. I strongly recommend his article "Good health is just a costly way to die".

Voluntary versus Regulated – An Alternative View

In contrast to the politically correct version of HIPAA, there is a contrary view that standards gain strength and acceptance in the market through open participation in voluntary organizations. Although messy, the process yields as fast an adoption of standards as possible and warranted by the problems they address.

The NCVHS is falling into the same trap, albeit on a grander scale, that other standards acceleration initiatives have. In order to move rapidly, arbitrary decisions, not consensus, cut the design and review phase to get “something” out. However, this merely shifts the complexity and problems from the front-end to the back-end of the process. Ironically the NCVHS subcommittee hearings laid out the case well. At two separate points the subcommittee heard how much HIPAA has accomplished since 1996 compared to HL7. HIPAA is done and HL7 is struggling to get Version 3.0 out. Or should we view this as HIPAA 1.0 beta release versus the third major release of HL7 in response to market requirements. Version 3.0 will be the first reference information model based HCIT standards, available in the next year or two, while HIPAA may still be trying to resolve problems in implementing transactions, privacy and security because they were found unworkable and impractical.

HL7, in particular, faces a Faustian bargain in the offing. Will it trade autonomy and self-direction for federal funds and legal mandates? It is an illusion to think that voluntary SDOs will not seek direction from an HHS that has the authority to make their standards mandatory. This is already occurring among the SDOs/DSMO in the financial standards domain.

Next Issue

In October we will report on the status of HL7 based on its Plenary Session that month. Despite its presumptive preeminence among SDOs, HL7 has a long way to go with Version 3.0. First balloting will be considered and we will have some sense of when an approved standard might emerge. We will also try to catch up on some of the general issues surrounding security, digital signatures and W3C standards. In December we will cover ASTM and IHE/DICOM. We will continue to track the course of HIPAA mandated standards in both issues. Please address comments and suggestions to Carla Smith at csmith@chim.org. Questions and other points of view and interests can be sent to Ed Larsen, erlarsen@erlinc.com who prepares the *Standards Insight* on behalf of the CHIM members.