



Standards Insight

An Analysis of Health Information Standards Development Initiatives

January 22, 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.

In This Issue:

| | |
|--|--------|
| Introduction | Page 1 |
| HIPAA Is Poised to Consume the HCIT Industry | Page 2 |
| The Privacy Rules | Page 2 |
| The Proposed Security Rules | Page 3 |
| Pivotal role of digital signature | Page 4 |
| The Joint SDO Meeting on Security | Page 5 |
| Background on Electronic Signature | Page 5 |
| The Meeting Itself | Page 6 |
| Bottom Line | Page 8 |
| Update from HL7 | Page 9 |
| HIMSS Preview | Page 9 |
| Is HIPAA good or bad for the HCIT industry? | Page 9 |

Introduction

This is the first issue of CHIM's *Standards Insight* for 2001. Its objective remains the same as last year's, to provide business analysis of the impact of standards on the industry's products and services. This issue will focus on how HIPAA privacy, security and digital signatures will redefine the industry's priorities. It includes a report on a joint meeting of standards groups on security.

We will also provide a status update on HL7 and a brief note on the upcoming HIMSS conference.

HIPAA Is Poised to Consume the HCIT Industry

Many sources cover HIPAA, why the *Standards Insight?* Standards under development are the future of HIPAA and HIPAA is the distribution channel for current standards. HIPAA mandates the adoption of selected interoperability standards. This trend, as we will see, will grow and extend into all facets of HCIT.

From the perspective of the healthcare information technology industry, HIPAA compliance is the responsibility of a covered party, i.e., a provider, health plan or clearinghouse, not of a vendor or service provider.¹ Why then the question is your product “HIPAA compliant” or more properly “HIPAA ready”? The question can be applied in regards to implementing specific transactions and codes, in regards to security features and in regards to digital signature support. We have discussed the transactions and codes last year after HHS published these regulations in final format.

The proposed HIPAA regulations for security and digital signatures are the rules that could turn the industry inside out. But to begin, we need to review the newly published privacy regulations.

The Privacy Rules

The final privacy regulations were published in the Federal Register on December 28, 2000. They are important, detailed requirements placed on covered parties (providers, plans and clearinghouses and their business associates) to protect individually identifiable healthcare information. The final rules extended their coverage from electronic data to all formats for using and disclosing protected health information. They require that a covered party obtain consent for standard terms of use and disclosure of the protected information. They permit the individual to request restrictions on the use and disclosure of their data. The covered party may also seek authorizations for additional uses. The covered party must track such use and disclosure. Besides the opportunity to create applications to keep track of consents, authorizations, restrictions and disclosures, the privacy regulations begin to set the requirements for “HIPAA ready”. They frame the security standards to which covered parties will be held in protecting individually identifiable data and in turn what features and functions they would expect in “HIPAA ready” systems.

The privacy rules generally state that a covered party may not use (within its own entity) or disclose to another entity protected health information except as permitted by these rules.

- Permitted uses and disclosures generally include those necessary to carry out treatment, obtain payment and conduct operations of the covered party
- But such use and disclosure must be the minimum necessary for the intended purpose.

¹ The exception is if the HCIT vendor is providing a covered service to a covered party. In fact unless the HCIT vendor is providing services relating to the operations of a covered party, it is not even a business associate. Access to systems with protected information for implementation and support purposes would be covered by administrative procedures and contracts.

- After obtaining consent, there is a general exemption from the minimum necessary and disclosure restrictions for the purpose of providing care by a provider.
- However, a covered entity must still adopt policies and procedures to restrict access to private healthcare information within its entity appropriate to defined roles and needs. The example is allowing nurses to access the entire medical record of patients on their ward during their shift. The implication is that they have no access at other times. What is more problematic is other employees from medical technicians, to medical records clerks, to admission personnel to housekeeping and how to develop policies and procedures to insure appropriate access to presumed subsets of a patient's protected information whether it is in electronic, written or oral form.

The privacy rules really set up the need for the security rules and the security rules will drive most of the HCIT industry change. We can begin to map the complexity with which a healthcare information system must deal: users in roles and different classifications of data for minimum necessary and permitted use implementations.

The Proposed Security Rules

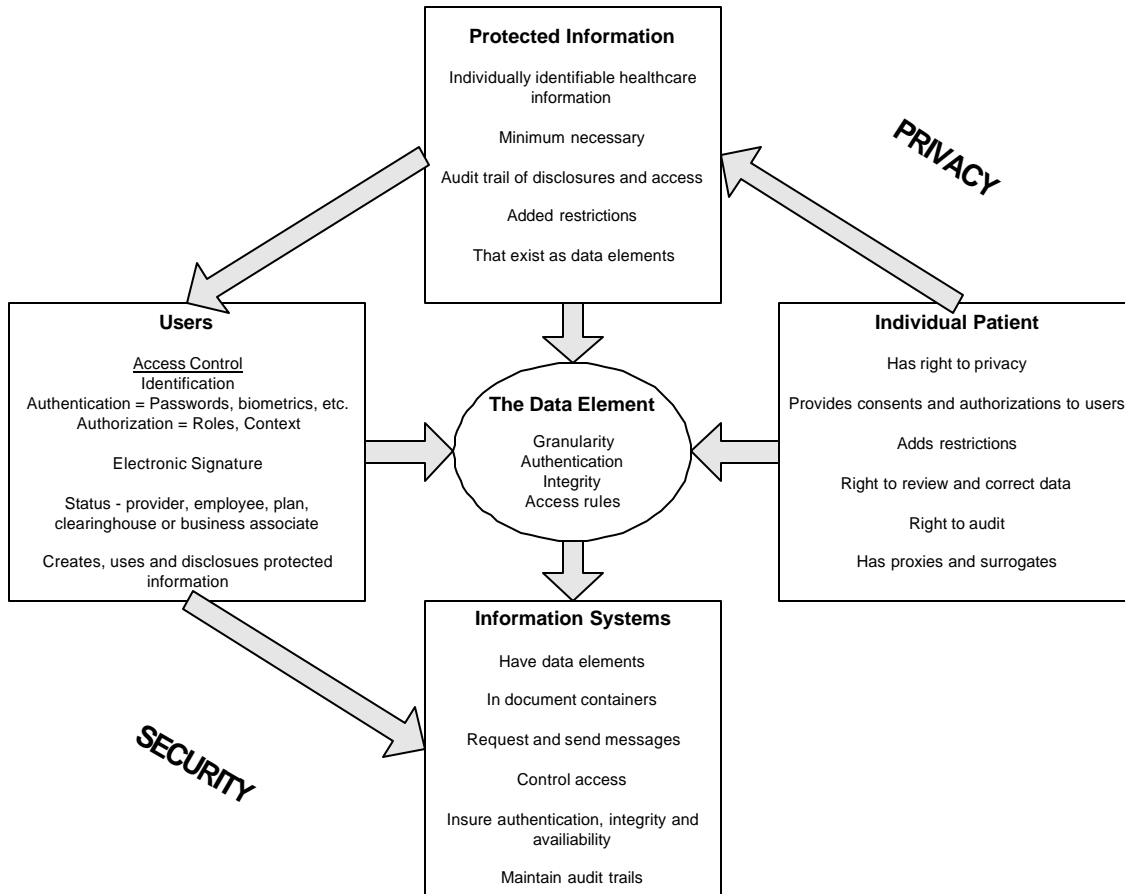
The timing of the final security regulations remain uncertain, particularly given the new administration that has given indication, in the different context of executive orders, of a desire to review recent rules and regulations. Some within HHS might feel that the privacy regulations themselves insure a heightened security effort among healthcare organizations. Certainly the final security rules will have to reflect the changes in the privacy regulations, particularly in expanding coverage to written and oral instances of protected health information.² It might be useful to briefly review the proposed rules.

The NPRM of August 1998 outlined the relationship of privacy to security. The former requires the latter. But in addition to privacy, security also insures data integrity and availability. HHS found that there was no single security standard available but that its regulation was intended to define fully the security requirements that covered parties must fulfill. Recall that the security regulations covered all protected data maintained by a covered party, whether or not the data was used in any HIPAA transaction.

The proposed security rules set requirements for administrative, physical and technical policies and procedures. The administrative procedures include the requirements to control access and maintain an audit, which are then described as part of the technical security services. These services add authorization and authentication for users and data.

The more far-reaching impact on HCIT is the need to design applications, data records, messages and electronic documents to be compatible with a complex, multi-level security framework. The framework of policies and procedures must be implemented to restrict workforce access according to individuals and roles to the minimum necessary data required for the purpose, notwithstanding the full access afforded care providers in some circumstances. External disclosure has the same standards plus a next level of complexity since it involves an independent entity. The privacy regulations also impose a requirement that any request for data be consistent with the minimum necessary for the purpose. The following matrix illustrates some of the system complexity.

²This would eliminate the exemptions for facsimile, voice mail, and other "oral" forms of communication.



Pivotal role of digital signature

Last summer it was widely reported that the electronic signature section of the NPRM would be omitted from the final security regulations. There were two rationales: that the initial transactions, to which the electronic signature standard applied, did not require electronic signatures and second, that the only acceptable technology, digital signature, was too immature to mandate. Time has passed and, in particular, it appears that the claims attachments and the next set of transactions will require electronic signature, creating a renewed urgency.

Independently HL7 found that its Reference Information Model did not explicitly define electronic signatures and authorizations, two elements needed in its clinical document architecture (CDA) requirements. Belatedly HL7 also recognized that such electronic signatures would be needed within messages, not just as part of the wrapper. Last fall at the ASTM E31 Committee on Healthcare Informatics meetings, Subcommittee E31.20 became concerned that HL7 was developing its own independent approach to digital signature in regards to its RIM and clinical document architecture. Given ASTM's existing digital signature standards and those under development, the subcommittee believed that HL7, rather than beginning a new and potentially incompatible approach to digital signatures for healthcare, should consider its experience and work products. Thus E31 sought to set up a meeting with HL7, an unusual event in healthcare informatics standards development.

HL7's need for and ASTM's experience with "signing" documents and messages and the major but uncertain role of digital signatures within the yet to be finalized HIPAA regulations prompted a joint meeting of the standards development organizations directly concerned with digital signatures in healthcare.

The Joint SDO Meeting on Security

HL7's Secure Transactions Special Interest Group hosted a joint meeting of interested Standards Development Organizations on Healthcare Security at its January Working Group sessions.³ Representatives of ASTM E31.20, of Accredited Standards Committee X12N and of the National Council for Prescription Drug Programs (NCPDP) presented overviews of their respective interests. Other representatives included members of EDIINT, the Veterans Administration, the Drug Enforcement Agency, the American Dental Association and National Center for Vital and Health Statistics. The last two are important HHS designated advisors on HIPAA and its future evolution.⁴

The meeting agenda began with two objectives:

- Developing standards for securing HIPAA healthcare transactions
- And establishing a basis for future cooperation between the SDOs on security.

As we will see the first objective morphed into a broader purpose, evaluating a single standard for digital signatures in healthcare. As a result digital signatures may play a pivotal and multi-faceted role in the security framework.

Background on Electronic Signature

An electronic signature is any electronic mark that can be used to show the intent of the individual to sign "something". Thus an electronic signature can be a scanned signature, a manual signature captured by a digitizer, as used by UPS, biometrics, passwords and tokens, or a digital signature, i.e., a public-private key pair⁵. An analogy can be made to a simple signature on a letter, a witnessed signature or a notarized signature. An electronic signature can also convey authentication of identity and intent. For example, biometrics creates strong evidence of identity, intent and authentication. Authentication is a necessary element in assuring non-repudiation. Besides authentication, as a signer, one wants to insure that one's signature is bound to whatever is signed and that the package is not changed. Thus data integrity becomes

³ Contact the co-chair Glen Marshall at Glen.Marshall@smed.com for further information.

⁴ It should be noted that the Designated Standards Maintenance Organizations, which includes HL7 and X12 but not ASTM, only analyze requests for changes and make recommendation to HHS for the transaction and code rules. The DSMOs responsibility do not extend to privacy and security regulations. In contrast the Secretary HHS must consult with and review recommendations by NCHVS. Hence this joint meeting was a significant industry forum.

⁵ A digital signature is based on use of a public and private key pair. The sender signs and encrypts a message or document using his private key. A recipient uses the public key, obtained from a trusted source, to decode the message. This insures that the received message is from the sender and that it has not been modified in transit. This methodology imposes overhead on systems and requires an extensive infrastructure to manage the keys or digital certificates. PKI does not inherently insure that only the intended recipient has the public key. Access controls are still required.

another element in electronic signature. Depending on how important the signature is in a transaction or document, some forms of electronic signature are much less desirable than others. Only a digital signature can be used to identify, authenticate, show intent, and insure data integrity and non-repudiation. Even here, if an individual gives out his private key, identification can be questioned. Hence one might need some form of biometrics identification and public-private key pair for absolute certainty. In the NPRM for electronic signature, HHS designated the digital signature using PKI as the only acceptable form for an electronic signature.

There are at least two prototypical use cases for electronic and digital signatures. One is as an alternative to a physical signature, a mark showing intent to attest and authorize. The other is as a security mechanism, such as in message transmission. The latter is easy to understand as an electronic FedEx package. One gives the package to FedEx who insures its secure transmission to another party who can be required to provide a return signature upon receipt. FedEx does not vouch for the accuracy or validity of the contents or signatures in the package, just that it was picked up from a location, was not altered in transport and was delivered to a recipient evidenced by a receiving signature.

Similarly within HIPAA there are two main applications of digital signature. The first is as a digital signature, which would be required for any designated transactions that required an electronic signature. The initial transactions finalized in August of 2000 do not require digital signatures. As noted, it is likely that the next set of transactions and claims attachment will require electronic signature. The second HIPAA usage of digital signature are in the Security NPRM where it is referenced as an acceptable technical security mechanism to insure authentication and data integrity. However, unlike in the case of transactions, the proposed security rules do not mandate the use of a digital signature whenever an electronic signature is applied, nor if digital signature technology is used as a security mechanism, no form is mandated.

Most of the HIPAA analysis and real world experience in EDI has been with the FedEx-like EDI application. Healthcare in particular and any industry in general have very little experience with electronic document process and management using digital signature, particularly within the enterprise's boundary.⁶

The Meeting Itself

Each of the key SDOs presented their perspective on use of digital signature and their standards.

- HL7 acknowledged that electronic signatures are not part of its version 2.x messaging standards. However, as it developed its Version 3 Reference Information Model and its Clinical Document Architecture, it found a need for electronic signatures for reports, orders and medical documents. It wanted such a "signature" to be part of any attributed statement, conceptually integrated not wrapped. Initially HL7 was considering the use of XML digital signatures, expected to become a standard by midyear. They are concerned

⁶At this point we do not want to raise the confounding issue of authorization, the use of digital certificates to convey privileges, credentials and authority. For example consider the electronic form needed to certify that a signature is that of a physician licensed in the state of California, board certified in internal medicine and with staff privileges at Cedars-Sinai. We will consider certificates, authorizations and infrastructure in a future *Standards Insight*.

about compounded documents and nested signatures and now are beginning to consider certificates. They also differentiated between a digital signature for the purpose of internal use and as part of a security wrapper for external messages.

- X12N has “primitive” standard methods for securing transactions. A sender can encrypt or sign a transaction or function within an X.12 wrapper. However, such signing is not interoperable outside of X12 or widely used. In all X.12 would prefer to use an existing security framework. Their proviso however is that it work with more than Internet Protocol, e.g., in older batch modes.
- The NCPDP has no electronic signature standard. In virtually all cases, state boards govern electronic scripts. Like X12N, NCPDP wanted to insure that any digital signature standard will support multiple, legacy transports. Since most NCPDP transactions travel on private networks and are charged per packet, the overhead of the digital signature was an issue.
- ASTM E.31 presented an overview of its approved standards (1762, 2084 and 2085) for electronic signatures covering policy and technology and the standards under development. These latter include:
 - ◇ Public Key Infrastructure Certificates
 - ◇ Directory attributes
 - ◇ Certification practices statement
 - ◇ Privilege management infrastructure
 - ◇ Implementing health information security programs
 - ◇ Risk assessment
 - ◇ Support for long term non-repudiation

In general ASTM E31 has focused on documents, not messaging like HL7. But unlike HL7 standards, ASTM E31 standards are not in widespread use. With HL7's evolution to documents and the need to include “signature and certificates” in the RIM, there is now potential opportunity to cooperate on interoperable standards for messaging and documents.

Other views particularly from the EDI domain were presented. S/MIME and PGP are two widely used, but incompatible standards for secure e-mail and Internet transmissions. Several industries, particularly natural gas transmission and the auto industry have developed standards for secure delivery of business data on the Internet, i.e., AS1 and AS2. However, these “standards” still require message profiles agreed to by trading partners. Moreover this experience was acknowledged to be substantially different from either the HIPAA use case or the internal document security instance. EDIINT transactions are still relatively fewer and of much higher value than are HIPAA transactions. EDIINT is used for inter-enterprise security and its infrastructure and response time would be unacceptable within a healthcare organization.

A key participant, Kepa Zubeldia of Claredi⁷, X12 and WEDI, provided insight into electronic signatures at the national policy level, specifically in regards to HIPAA transactions and security requirements. While last summer's decision to delay electronic signature rules might have made sense then, time has passed and ironically the security regulations themselves have not been published. However, claims attachments and a next set of EDI transactions, particularly involving patient consent, will need electronic signatures. Thus there is some pressure to revisit electronic signatures.

The meeting, at the suggestion of Dr. Zubeldia, focused its efforts on to recommending a digital signature standard and determining if a single digital signature standard might be adopted to cover not only transactions. In other words a single standard for the FedEx scenario, which would apply, if possible, to all of the other applications of digital signatures as mentioned in the proposed security rules. In fact NCVHS is inviting testimony in early February from the SDOs on such an agreement, if not for a single digital signature standard then to the commitment to evaluate the possibility. This could be interpreted as Washington's attempt to get "industry" to buy into a single standard. This would pave the way for HHS to issue the delayed electronic signature regulations in time to support new transactions and claims attachments.

There was muted agreement that such a single standard would be desirable, *if feasible*. The consensus, such as it was, did not reflect official or consider positions of the SDOs themselves, of course. A representative from ASTM stressed the different levels or use cases of digital signatures within healthcare organizations. Considering how clinical documents are created and "signed", a digital signature may not be appropriate for all circumstances. It should be noted that a digital signature once applied makes the document immutable, i.e., for data integrity and non-repudiation purposes. Thus the infrastructure and overhead to manage "signed documents" could become quite large. For example, are nursing notes "signed"? Is each lab value "signed"? Certainly the security regulations would expect such data to be protected and authentic but there are alternative secure methods, particularly for use within an enterprise's boundaries. One could set up a system where only some data or documents are digitally signed and the others are "secure". Add a layer of complexity to the matrix. Consider adding where and when one adds a digital signature to a data element.

Bottom Line

The meeting highlights the difficulties that healthcare information systems vendors face in "being HIPAA compliant". Those involved in the HIPAA transactions have a more straightforward implementation requirement. There will be some specified digital signature standard for the transactions between covered parties. The problem is for those vendors that have software that is used to manage messages and documents containing patient information within an enterprise. These will be covered by security rules. While the general privacy rule permits flexibility in "using" such information for patient care and organizational operations, there still must be security. The proposed rules outline technical security requirements, which must be supported by software, including access control, identity and authentication, authorization, encryption and data integrity. If a digital signature is used, it will presumably have to meet whatever standard is adopted, at least as the trend exists today. What we do not know is at what level of data granularity and workflow this type of security must be applied.⁸ If a digital

⁷ www.claredi.com

⁸ The impact on software applications is enormously different if each must manage access controls and authorization or if they can assume some central service passing only authorized users. This is obviously much more complex than single sign-on. There is some experience from

signature is used as the means for all access control identification, authorization and insuring data security, then a new, high overhead system must be developed. Data must be signed at a granular level of creation, not at some later point, retroactively imposing "security". If digital signatures are used now only where formal signatures and attestations are required, then we will have a two level system: one password based with unencrypted data and messages and a PKI-encrypted based. If a digital signature is only added to documents at some benchmark point, e.g., at end of a procedure, shift or discharge, then who will attest to the validity of all the intermediate data? How do you implement a secure system halfway through the process? Physicians in particular are very sensitive to their role in "validating" others data with their signature.

The most immediate HIPAA question for the HCIT industry is the single digital signature standard. Is a standard that is appropriate to meet the requirements of EDI and external transactions suitable for an internal security framework? Given the clearer, near term need for a digital signature in upcoming transactions and claims attachment, the momentum is clearly with the EDI side. Moreover, given the new and yet unproven cooperation between the SDOs, particularly HL7 and ASTM, there may not be a focal point to develop and articulate the use of digital signatures as part of internal operations and security.

Update from HL7

HL7 held its January Working Group meetings earlier this month. Most of the sessions were focused on moving its Version 3.0 standard forward. Like all development efforts, it becomes increasingly more difficult and time consuming to add and change the RIM and its methodologies to derive messages and documents. Each of the Technical Committees has responsibility for some aspect of the domain that is captured in the RIM and represented in messages. Thus more and more time is spent in detailed coordination and reconciliation. It is also clear that HL7's decision to be an international initiative has added another layer of complexity as it seeks to accommodate diverse language, workflow and regulatory practices.

Version 3.0 exists as the RIM, its associated message generation methodologies, the XML based messaging implementation guide, clinical document definitions and some associated artifacts. Some problems, such as the lack of security entities or actions in the RIM have a major impact across most deliverables. Other problems such as the decision whether to use XML DTDs or schema in Version 3 messages can be isolated at a lower level. Others represent real conceptual challenges, such as how to handle local extensions, e.g., Z-segments. While the intent of Version 3.0 was to create a plug and play standard, the reality is that individual organizations will have data requirements not captured in the RIM. The resolution could be anything from a tight ban on any extraneous data, adding local profiles, using name value pairs or creating a Z-RIM.

HL7's late arrival to security issues will slow Version 3.0 and may impact CCOW's direction. This is true even without consideration of digital signature as discussed earlier.

HIMSS Preview

Two very different standards initiatives will be demonstrated at HIMSS: HL7 and Integrating the Healthcare Enterprise (IHE). HL7 will demonstrate elements of Version 3.0 including XML

CORBAMed's RAD (Resource Access Decision) with policy evaluator services. This area will be considered more completely in the next issue, along with certificates.

messages using DTDs and use of the CDA. They will have approximately 10 vendors involved. They will also demonstrate CCOW and present overviews in a small theater setting. HL7 is trying to address an internationally accepted, comprehensive framework for healthcare information standards. All of this will occur within a 20 by 30 booth.

We have previously reviewed the IHE Year 2 demo, initially shown at RSNA. IHE is a joint acceleration project of RSNA and HIMSS. It is heavily supported and funded by the imaging modality and radiology information system vendors. It will have a featured theater and demonstration area several times larger than HL7's with 30 plus participating vendors. As noted it will almost exclusively focus on interoperable workflow within an imaging department.

Is there anything wrong with this picture?

Is HIPAA good or bad for the HCIT industry?

It certainly depends on how complex the security framework becomes. It probably depends on one's products and services. Certainly the privacy and security regulations will redirect spending priorities. Money for new applications will be directed towards insuring current applications can support whatever security framework is required. Probably good for those with large installed bases and bad for those depending on selling new applications. Y2K redux! Some new technologies, such as wireless, may see some repercussions in meeting industrial strength security requirements. Ed Larsen, the author of *Standards Insight*, will present "How HIPAA Privacy and Security Regulations Will Shape the HCIT Industry" at CHIM's Member Luncheon, on Monday, February 5th, during HIMSS. See www.chim.org/Education/2001MemberLuncheon.asp for further information and to sign up.

The *Standards Insight* is prepared by Ed Larsen (erlarsen@erlinc.com) exclusively for CHIM members. Please contact Ed or Carla Smith (csmith@chim.org) with any questions or recommendations for the *Standards Insight*.