



# Standards Insight

## An Analysis of Health Information Standards Development Initiatives

*October 19, 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

OVERVIEW .....	2
PRIORITIES REVISITED .....	2
SECURITY .....	3
Digital Signature .....	5
HL7 .....	6
Version 3 .....	7
CCOW.....	8
Structured Documents.....	8
MISCELLANEOUS NOTES .....	10
W3C .....	10
ebXML.....	10

## OVERVIEW

This issue of the *Standards Insight* addresses our two planned topics: security and HL7. However, September 11<sup>th</sup> and its aftermath are causing healthcare organizations, as are we all, to revisit information system priorities. Security, with or without the impetus of HIPAA<sup>1</sup>, has risen to the immediate attention of executives and boards. While HIPAA Privacy and the Standard Transaction rules are not yet delayed, they have become marginally less important priorities. We will look at this shift. As noted in the last issue of *Standards Insight*, the National Center for Vital and Health Statistics (NCVHS), under mandate from the original HIPAA legislation, is beginning to examine interoperability standards for a patient medical record. Our initial experience with bioterrorism raises the priority of ready exchange of clinical data and of the national healthcare information infrastructure. Not coincidentally, HL7 has found purpose for its Version 3 and broadened its mission to include extending its standards to an electronic health record.

## PRIORITIES REVISITED

The terrorists' attacks on September 11<sup>th</sup> jolted the nation. They highlighted the need for emergency preparedness and disaster response capabilities among healthcare providers. The ongoing sinister spread of anthrax puts healthcare providers on the frontline and underscores the importance of the public health infrastructure. Both of these new priorities are information intensive. The former are elements of a well-structured security and contingency plan. The latter requires a seamless flow of information from physician offices, emergency departments, state health agencies, the Center for Disease Control and testing laboratories. A basic requirement for information security and public health infrastructure is interoperability. In fact, the CDC is currently trying to upgrade its national networking, potentially based on secure HL7 messaging.

It is plain to all that security and contingency planning have become very important priorities not only to CIOs but, more importantly, to health care organizations' chief executives and boards of directors. This shift to the executive suite will broaden and deepen security initiatives beyond information systems. We will discuss this impact on security in the next section. Here we note the inverse: the impact on implementing the HIPAA Privacy and Standard Transactions rules.

We have noted before that HIPAA Privacy and Transaction rules involve high, front-loaded costs for healthcare organizations. Economic benefits accrue later and probably not to the healthcare organizations but to us the ultimate payors. HIPAA implementation uses discretionary funds. Also inherent in these costs is use of key management and information systems resources. Our current war on terrorism changes national healthcare priorities. The national healthcare information infrastructure is needed to support public health. This will require new spending and accelerated interoperability standards. Healthcare organizations are being mobilized for handling external attack and mass casualties. On the margin a relative shift in priorities for spending and resource use to security and emergency preparedness must reduce efforts elsewhere. The AHA has already been before Congress presenting its needs for additional funding. It is likely that the Privacy and the Standard Transactions implementations will be that "elsewhere" and their compliance date will be delayed.

The Privacy rules do not look quite as urgent right now.<sup>2</sup> In fact while the administration has summarily decided not to move towards national identity cards, there is no doubt that privacy rights and national security involve trade-offs. Currently proposed legislation on consumer privacy looks suspiciously like safe-harbor and hold harmless legislation for enterprises that collect personal information rather than an extension of privacy rights. In any case the Privacy

---

<sup>1</sup> As is our custom, HIPAA is used to mean the Administrative Simplification sections of the Health Insurance Portability and Accountability Act of 1996 and resulting HHS regulations.

<sup>2</sup> In fact Congress has asked HHS to investigate whether the Privacy rules will interfere with patient care.

rules under paragraph 164.514 clearly permit healthcare organizations to disclose protected health information for public health and law enforcement purposes without the need for consent or authorization. Use of the various public health and law enforcement and intelligence agencies create more interesting privacy questions. In our new war, the Privacy rules neither advance nor hinder the effort, but they add costs and consume key resources.

The Standard Transactions rules are further along in terms of implementation, i.e., sunk costs. Nevertheless there remain strong proponents of delaying the compliance date, now just a year away. The national governors association has renewed its call for a delay, claiming that the states do not have the funds for HIPAA and other healthcare and welfare claims in view of declining tax revenue and new homeland defense requirements.

While it is difficult to sort out the overall validity of these trade-offs, it is clear that the slowing economy, perhaps tipped into a recession by the terrorism, will reverse the profit recovery of healthcare providers. Healthcare is a lagging industry in the business cycle. Rising unemployment reduces health insurance coverage. Rising premiums drive employers to reduce benefits and shift costs. Falling tax revenue squeezes Medicare and Medicaid spending. Bottom line, healthcare providers will have less funds to devote to discretionary projects.<sup>3</sup> *Ultimately, the economy and changing national priorities will likely delay HIPAA implementation.*

## SECURITY

In the aftermath of September 11<sup>th</sup>, the proposed HIPAA security rules do not appear either onerous or sufficient. In fact, information system security initiatives will move forward rapidly with or without final rules from HHS. However, security has become an enterprise endeavor of executive management and their boards, not just an IT effort managed by CIOs. The focus will be on emergency response, disaster recovery and contingency operations covering staff, supplies, facilities, communications and not just IT. Healthcare organizations must be prepared not only to recover from disaster but also remain a first line responder. Thus high availability information and communication systems will become the highest IT priority.

But we need to step back from solutions to re-examine the problem. Security begins, not with technology, but with an assessment of risk, or as we now understand threats, and then an analysis of the costs of reducing those risks. Before September 11<sup>th</sup>, most IT risk assessments focused on internal threats, since current and ex-employees accounted for most security breeches. External threats were seen as random attacks from computer virus, denial of service and hackers. Privacy or confidentiality, not availability and data integrity (the three objectives of HIPAA security rules) was seen as the defining objective. Now we are faced with new situations in which system availability and external threats rise in relative importance.

Making the trade-off between risks and costs is one of the most important decisions an executive team makes. They then formulate the security policy, which is directed at people, their roles and responsibilities and their permitted activities. Among these are their access to and use of information and systems. To implement the policy we develop procedures.

As we painfully observed in the terrorist attacks, the most immediate security risk is physical. Thus physical security of people, buildings and technology is a baseline. Hospitals have security procedures to limit physical access to patient care units and other sensitive or vulnerable areas. Physical security is similarly needed by information systems. Physical access to computers and networks can defeat most of the next level of technical security measures.

Finally we configure the information technology itself to support secure policies. This includes restricting access, limiting authorizations, maintain audit logs, backing up, encrypting and protecting data. Technical security is not only applied to workstations and servers, but involves

---

<sup>3</sup> It should be noted that hospitals non-operating funds from investments have also been negatively impacted by the stock market declines.

special considerations for networks. These include firewalls to isolate internal and external networks.

Nestled within the proposed security rules is the need to have contingency plans and back up and recovery functions. These take on greater urgency both in terms of the direct threat to a hospital computer system, but more so to the need to have access to computer systems during large-scale emergencies and disasters.

Generally we can divide IT security plans into two realms: the closed, tightly coupled system internal to an enterprise and the open, loosely coupled system not controlled by the enterprise. The former realm can depend on strong policy and procedures and physical security measures in addition to technical measures. The latter, e.g., the Internet, requires more extensive use of technical measures, such as strong authentication and encryption. Each realm creates its own interoperability issues in maintaining security across diverse systems.

There are five interrelated security functions laid out in the HIPAA NPRM.

- Access control including:
  - User identification
  - Authentication
  - Authorization
- Audit
- Data authentication and integrity controls
- Data and system availability
- Network security

Based on the risk assessment and policies and procedures, one would select technical methods appropriate to the type system: open or closed. Thus internal access control most probably will depend on weak methods such as unique ID and password (the HIPAA minimum). External access control, e.g., dial in access, might more appropriately require stronger authentication such as digital certificate/token. Similarly internal data is likely to be protected by access control and audit trails whereas external data may require these and encryption. Each of these choices involve cost and convenience trade-offs. Highly secure, encrypted systems will be more expensive and harder to access and use.

Interoperability issues arise whenever heterogeneous networks and applications come together. Lower level security, e.g., at the network packet or port level, can be based on general IT standards. Stepping up, UNIX and NT based networks support access controls and directory services for some levels of authorizations. However, in most cases individual applications maintain privileges for their authorized users. If one is willing to manually configure and maintain these lists and privilege sets on each application, one avoids the interoperability problem. However, when clinical data moves between applications, e.g., across an HL7 interface, significant issues of maintaining data integrity and a chain of trust arise. For the most part we ignore the problem within a closed system relying on each application to provide valid data to the others. Systems are designated as possessing data of record and in any event most long-term storage occurs in the form of printouts and paper forms.

In some cases, we have adopted single log-on services, more for convenience than to enable interoperable access controls. There are proposed open standards, such as OMG's Resource Access Decision (RAD) that would provide a centralized, fine-grained access control service for subscribed applications. The minimum necessary provisions of the HIPAA privacy rule add a further dimension to maintaining access control. It may not be sufficient for a central service or application to attach privileges to users without the context of the individual patient. Finally, to create an integrated and comprehensive security system, these functions must interoperate with

other functions as well as among the applications. For example an audit trail<sup>4</sup> is an essential element for checking access control and for maintaining data integrity.

*We note in closing that interoperable security standards will become the major impediment to an electronic medical record. If healthcare informatics SDOs do not coordinate the solution or simply adopt general-purpose solutions from the e-business world, we may have a very unusable or very insecure EMR system.*

### **Digital Signature**

Interoperability problems really converge upon digital signatures. This unfortunately named technology does act as a strong form of an electronic signature. However, it is equally a powerful security mechanism for implementing access control and maintaining data integrity. We have described the technology and policy issues concerning digital signatures in past *Standards Insight*.<sup>5</sup> The two roles, electronic signature and security, are confounding when applied to clinical document processing. For example, physician orders and reports are “signed”, many chart entries are “initialed”, and results are “validated”. In the course of a hospital stay, many different care providers “sign” components of a medical record. Digital signing creates and encrypts each of the “signed” entries/documents. The medical record is the compound document of all these digitally signed entries. If used in this manner, signature and data are tightly bound. In contrast simple electronic signature, as described by JCAHO as a keystroke or password, may indicate who made the entry (access control) but, on its own, cannot insure that the data was not changed. Here one must rely on underlying system security and audit trails. Separate authentications of signature and data become an issue over time and in legal disputes. However, it is a much simpler, low overhead computing environment. Thus most internal systems, i.e., the closed network within an enterprise, use the less rigorous electronic signature/single factor identification method. As envisioned by the proposed HIPAA electronic signature rules, digital signatures were to be required for the standard transactions and attachments sent between enterprises. Here, because the signature/data is exposed to an open network, the security characteristics of digital signature, e.g., the electronic version of FedEx, are necessary. In most cases, however, the content of the electronic FedEx envelope is a compound document produced from the weaker forms of electronic signature – signed by medical records as a true copy as produced by their business rules and documentation process.

The internal closed or external/open system issue applies to signatures (which inherently implies unique identification and entity authentication) and to authorization or permissions. Local, closed networks, as one would find in a hospital or physician office, can rely on strong administrative security policies and procedures and, in some cases, physical security. Thus weaker technical security mechanisms are often used. Specifically single factor identification/authentication, such as ID and password, are sufficient. Stepping up in complexity out-of-band or symmetrical key using a trusted token server might also be used. These internal systems can be expected to provide a user access list or service since all users are known to the system. The in-band analog cannot depend on the same administrative policies and procedures (although all covered entities are expected to develop these). Here an asymmetrical key pair is bound to the message. Moreover there is the problem of user ID and authentication interoperability between two separate enterprise systems. Inherent in digital signature, is the public key infrastructure (PKI) in which independent, trusted certificate and registry authorities exist to provide interoperability of digital signatures.

We noted that authorizations also complicate digital signatures. The digital certificate can carry attributes, such as credentialing and privileges, in addition to identity. However, this greatly complicates the real-time authorities that must update certificates. Out-of-band authorizations are currently managed at the application level, e.g., each application has a list of users and what they

---

<sup>4</sup> There are at least two audit standards, one from HL7 for audit messages and one from ASTM for audit records. While they need to be reconciled they can be a basis for collecting event data from applications into a central service.

<sup>5</sup> Refer to January 22, 2001 issue. Also see update in May 25, 2001 issue.

can do in that application. In-band authorizations must depend on the certificate or some external directory service. Again we are in danger of confusing authorization and security. If a system manages authorization separately from the signed activity, e.g., physicians are allowed to enter an order because they are on the order entry access list, then the only assurance a later third party has that an individual that entered an order was authorized is external to the order. Since a digital signature has the capability of carrying authorizations, it can be used to package signature, activity and authorization in a single secure record.

HHS and NCVHS would like to find some electronic signature standard both to enable new HIPAA standard transactions and claims attachments and to support a future personal medical record standard. Of course, such standard must be interoperable across diverse systems and enterprises. It would be desirable, in a chain of trust sense, that the standard was used internally, at the point of data creation, as well as externally. Such standard must be technically neutral, scalable and reasonably cost effective. It must be adopted in coordination with the Secretary of Commerce, who has broad interest in e-signing. Such a standard does not exist.

That is not to say that various standards for electronic and digital signatures do not exist. ISO X509 sets forth the digital signature/PKI standard. ASTM describes healthcare electronic record and signature requirements in its standards E1762 and E2084. The W3C is moving a XML based digital signature standard forward. Microsoft Hailstorm and Sun sponsored Liberty are general implementations and de facto standards. DICOM is planning a digital certificate standard to be used by all digital imaging devices to "sign" their studies. HL7 has remained relatively disengaged and now agnostic as to the security of its messages. The Version 3 Reference Information Model Encapsulated Data types can accommodate electronic/digital signatures and certificates. However, the security standard, method and implementation are viewed as external to HL7. This will become an increasingly painful view as security and signature become a determinant of messaging interoperability.

The Multi-SDO Digital Signature Project has gathered a preliminary set of use cases, primarily for in-band inter-enterprise cases. It may be stalling in signing up participants for an interoperability demonstration, targeted at next year's Toward the Electronic Patient Record (TEPR) conference. We believe this is at least a function of the relative diversity of use cases and application domains represented by in and out-of-band systems and the interrelated complexity of signatures, authorizations and security.

Look for a two-tiered system, internal and external system focused. Internally, electronic signature will be a part of security services, such as OMG RAD. Externally, digital signature will be PKI based and part of a national healthcare information infrastructure.

## HL7

HL7 has finally discovered a marketable reason for Version 3 - the electronic health record. Nominally Version 3 represented a solution to the primary problem of Version 2.X, the large amount of ambiguity and site specific implementations. Version 3 is to tightly define message usage, structure and content.<sup>6</sup> To accomplish this near "plug and play" objective, HL7 developed an extensive reference data model and message construction methodology. Although there are shortcomings discussed below, Version 3 clinical and administrative messages are likely to meet these interoperability objectives.

And this brings us to the great pretense among HCIT standards development organizations (SDOs) that there is a fundamental difference between data in motion (messages) and data at rest (medical records or documents). This pretense justifies the duplicative and overlapping work of ASTM and HL7 and to some extent – DICOM. We have multiple standards for describing the same essential medical data depending on if it is in a medical record, a structured report or a message. Granted that there are differences but not at the medical data concept and content

---

<sup>6</sup> Content in terms of controlled vocabulary depends on use of external code sets, such as SNOMED or ICD 9, that are registered with HL7.

level. Moreover, if interoperability is the goal, as it is for HL7 and for the NCVHS PMR recommendations, then message and document merge. If information in a document cannot be sent to another application there is no interoperability. Moreover if the document always is a superset of the message, then there is no interoperability since some data cannot be packaged in a message. In most cases it is the message that defines interoperability and content of the document. The data in the former may exist transiently and the latter may persist but the former must sum to the latter. That implies that the message must carry the context for use in a medical record. More to the point, the HL7 reference information model (RIM) can be used to derive documents as well as messages.

Possibly prompted by the NCVHS hearings this August<sup>7</sup>, the HL7 board elected to expand its mission to include electronic medical records standards at the recently completed Plenary Session. The decision was more pragmatic than strategic. Besides the NCVHS stimulus<sup>8</sup>, HL7 responded to international efforts to apply or map HL7 to different electronic health record needs. In fact HL7 set up a new Electronic Health Record special interest group (SIG) but this moves in a different direction discussed below. The Structured Document Technical Committee is deep into defining medical documents based on the RIM. It was apparent that HL7 either needed to embrace these medical document initiatives or forever restrict itself to the world of messages. If the RIM and the registered code sets represented 70 percent of the work effort for an EMR, why should HL7 turn away from the last 30 percent? If the HL7 membership has the expertise and interest to move to an EMR standard, should HL7 encourage them to go elsewhere? *If HL7 did not seize the EMR opportunity, then ultimately the RIM and the derived messages would be replaced by a model supporting the HIPAA regulated EMR.*

### **Version 3**

We have discussed how Version 3 will morph into an electronic medical record standard. Currently it is a fine-grained, tightly defined clinical and administrative message specification derived through defined methods from the RIM. Its target implementation is in XML, using schema not DTDs. It incorporates by registration, external vocabulary code sets. It is designed to be conformance tested.

The first ballot, conducted prior to the Plenary Session earlier this month, failed. This was not unanticipated given the scope and complexity of the endeavor. However, the ballot effort exposes some of the problems that HL7 faces. First, the RIM must be viewed as a massive effort – a comprehensive healthcare information model. In fact, the RIM development process became so complex as it modeled different domains and functions that the technical leadership simplified it by creating fractal like Refined Message Information Models (RMIM). RMIMs match up with the reality of the domain and functional committee structure within HL7. These technical committees and SIGs have domain or functional expertise (as well as internal political interests) necessary for providing content to the model. Having everyone work on everything in a single model was unwieldy and unproductive. We will now see how decentralized model building works. Coordination and interdependency between the committees will strain the organization. At the least this change created documentation problems and confused the voting membership. It is expected that these operational matters will be resolved for the next ballot, scheduled for February.

The confusion factor notwithstanding, few substantive issues appear to have been raised in the negative ballots. This reflects the frustrating strength of a consensus based SDO process. Most of the key issues were debated and resolved before any standards were decided. However, the evolution of Version 3 and the RIM has raised new issues. For example, how should one instantiate messages in a closely coupled system (with shared identifiers) versus a loosely coupled system (where identifiers must be detailed in the message itself)? Change and

---

<sup>7</sup> We covered this in the last *Standards Insight* dated August 27, 2001. We will analyze the October NCVHS hearings from users and vendors in the next issue.

<sup>8</sup> Woody Beeler presented on behalf of HL7 – indicating its official interest in being considered as a PMR standard.

localization had emerged as major challenge but HL7 is beginning to get a handle on change management in the context of the RIM. In particular there is a desire to restrict changes to the RIM and its data types but support extensions through new message types, attributes and templates. We have already noted the lack of intrinsic security within HL7 messaging and documents. Finally given the scope of Version 3 and the RIM and the extent of international participation, HL7 will continue to bump into other standards initiatives, organizations, and turf.

## **CCOW**

CCOW remains a well-marketed enigma. Its function, visual integration of diverse applications on a single desktop, is conceptually valuable if not essential in typical hospital system environments. It maintains a common user (single sign-on) and patient context. It can be used with both traditional Windows clients and on Web server based applications. It is widely supported in RFPs but remains narrowly implemented. Why?

First, the upside: it is a useful selling tool in a heterogeneous systems environment. Even vendors of comprehensive clinical systems, such as Cerner or IDX, are likely to be complemented by specialty or niche systems. While back-end data interfaces may let the core application present data from such niche systems, at some point users must go into the niche system. Specialty systems, such as automated drug dispensers, anesthesia records, ECG management, and all the PACS and imaging systems are primarily accessed through their native user interface. This is where CCOW shines.

On the other hand CCOW is not inexpensive when deployed over all workstations and servers. Financial justification may fall to the new niche vendor rather than to the incumbent core system. The latter major HCIS vendors often have some proprietary "context" manager or Web portal strategy for visual integration or a comprehensive clinical data repository to support a common user interface.

Finally CCOW is not highly secure in a period when user access control is rising in importance. While CCOW, as part of a "single sign-on" can pass identity certificates to applications, it is up to each application to manage access lists and privileges. This distributed security model, while less technically complex, is the antithesis of a centralized security service and system administration. Moreover, CCOW and its participating applications are relatively open to rogue applications and spoofing. Thus within today's environment, CCOW does what it does well but that is not enough. *As hospitals look at the broader issue of user access control, minimum necessary use, privileges and audit trails they will look for a more comprehensive solution. That such a solution does not exist will not add to CCOW's appeal.*

## **Structured Documents**

Structured Documents is the technical committee remaining after the XML SIG was split off. As noted the former focuses on documents, using XML, while the SIG focuses on applying XML technology to messaging. Its Clinical Document Architecture (CDA) Level One is now an ANSI certified standard.<sup>9</sup>

The CDA describes documents comprised of header and body definitions for three levels of documents. The definitions are based on the RIM. The CDA includes nested containers, compound documents and families of documents. A clinical document exhibits functional requirements not found in traditional HL7 messaging:

- Persistence – continues to exist in an unaltered state
- Stewardship – maintained by entrusted entity
- Potential for authentication – assembled with intent for legal authentication
- Wholeness – authentication applies to whole and not to portions without full context

---

<sup>9</sup> Incidentally this makes it eligible for inclusion in future HIPAA mandated standards.

- Human readability

Well before the HL7 board expanded its mission, the CDA was far down the path from messages to documents.

As noted earlier, the Board created a new Electronic Health Record SIG. The EHR SIG is primarily focused on an ambulatory record. Specifically the UK affiliate wants to see if it can use HL7 messaging to create an EHR for general practitioners. Initially it may base its efforts on Version 2.4 messages, which are in wide use, rather than Version 3 or the CDA. We will see how this evolves and whether it comes back into the HL7 mainstream.

#### What is an EMR?

*We should note that one of the continuing controversies within standards groups as in HCIT generally is the definition of an electronic medical record. Many SDOs and groups have a stake in this endeavor. Although the 1991 IOM publication of "The Computer-Based Patient Record" is a convenient benchmark, it neither represented the beginning nor does it reflect current understanding of a CPR. Fundamentally the electronic form of the medical record is an analog to current paper based records plus. A medical record is created by every healthcare provider for each individual patient as the business record of the provider. The record is populated with charting for each encounter or episode between the individual provider and individual patient. Thus there are medical records in hospitals, in physician offices, in home care agencies and many other healthcare organizations. Paper based, they are usually not integrated and often not complete and available from a filing system. Because hospital inpatients had the most complex records and the most IT infrastructure, most computerized patient record (CPR) development focused on this application. However, as computers became more widely applied in outpatient care settings, patient record systems evolved. Although not rigorous in definition, outpatient systems were often referred to as electronic health records (EHR). As hospitals tried to evolve into integrated delivery systems, the CPR/EHR or electronic medical record (EMR) unified all of a patient's data, irregardless of encounter type, into a single longitudinal record. The CPR/EHR/EMR was often placed in a clinical data repository (CDR). Cross patient data slices were moved to a data warehouse for analysis. More recently some Web sites have begun to offer personal health records (PHR). The latter, while "unofficial", centers the record on a patient, not a provider organization. The NCVHS wants to develop standards so that patient data can be moved easily between these various records and repositories. For some reason they call their standards effort the patient medical record (PMR). Interoperability might first start with a standard naming convention.*

*HL7 remains the market leader in healthcare informatics standards. Although its membership revenue is flat and total revenues, absent a VA grant, were down this year – partly reflecting reduced meeting participation following the terrorist attack, HL7 participation remains near record levels. It has embraced clinical trial standards in conjunction with CDISC (Clinical Data Interchange Standards Consortium). It continues to add international affiliates, now up to 18, both a compliment and a challenge for an American National Standards body. The decision to expand its mission, though necessary, will represent an ongoing challenge as it on the one hand tries to focus on its traditional messaging role and on the other the RIM/EMR role.<sup>10</sup> Diversity in*

<sup>10</sup> HL7 has recognized the importance of its core messaging by announcing ongoing support of its Version 2.x, which is widely implemented throughout the world. In fact, HL7 is proposing Version 2.4 as an ISO standard. The board has clarified that it is not HL7's intent to force users to move from functional Version 2.x messaging to Version 3.

*its members interests, while distracting, is probably the greatest assurance of HL7's continued pre-eminence as a voluntary, consensus based SDO. The danger to HL7 is to become a narrowly focused acceleration initiative, whether to win the NCVHS prize or to stay ahead of the "XML barbarians"<sup>11</sup>. There are all too many examples of failed acceleration initiatives that attempted to ignore complexity for speed.*

## MISCELLANEOUS NOTES

### **W3C**

We had hoped to look at W3C activities in greater depth since HL7 as well as other healthcare informatics SDOs, such as X12, rely on these standards. We will only note the controversy surrounding reasonable and non-discriminatory (RAND) versus royalty free licenses. W3C is proposing a new policy that would allow it to adopt as W3C standards proprietary or patented work under non-royalty free licensing terms. *This has historically not been done within the Web community and will present a problem for other SDOs, such as HL7, which incorporate these RAND standards within their royalty-free construct.*

### **ebXML**

ebXML ([www.ebxml.org](http://www.ebxml.org)) is a joint initiative of the UN/CEFACT and OASIS to create an open infrastructure for electronic business using XML. As such it specifies existing standards to be used within a layered framework extending from the business process down to the actual message service. It specifies W3C and other open standards rather than creating new ones. While open, ebXML is not neutral. It competes with Microsoft and IBM sponsored technologies such as SOAP and UDDI.

HL7 has endorsed ebXML messaging services (layer 5) and conducted a proof of concept demo in Vienna last May. This involved using ebXML as an envelope for HL7 messages and CDA reports. There is an ongoing effort to try to align HL7 artifacts such as the RIM and repository with other ebXML layers. ebXML could provide the standards for providing external services and functions, such as business partner agreements and registries, needed for inter-enterprise HL7 messaging.

*It is not clear how important ebXML will be to healthcare informatics. It may be useful in the supply chain world. It might be an alternative model for NCPDP scripts and for X12 based financial transactions, although eventually these would wind up within the HIPAA arena. ebXML would be more important within the context of a national healthcare infrastructure rather than as enabler of "private" HL7 clinical messaging between different providers.*

## NEXT ISSUE

In December, the *Standards Insight* will cover results of the ASTM Fall meeting, DICOM and the "Integrating the Healthcare Enterprise" initiative from RSNA, and updates on SNIP and the progress towards implementing the Standard Transactions. Please address comments and suggestions to Carla Smith at [csmith@chim.org](mailto:csmith@chim.org). Questions and other points of view can be sent to Ed Larsen, [erlarsen@erlinc.com](mailto:erlarsen@erlinc.com) who prepares the *Standards Insight* on behalf of the CHIM members.

---

<sup>11</sup> The latter phrase is attributed to the tongue in cheek remarks of Dr. Stan Huff, current chair of HL7, at the Plenary Session.