



Standards Insight

An Analysis of Health Information Standards Development Initiatives

March 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

Introduction	1
HIPAA at HIMSS	2
HIPAA Administrative Simplification	4
HIPAA Outlook	6
Outlook for HCIT Industry	8
Bottom line	9
Next Issue	9

Introduction

This issue of the *Standards Insight* will focus on HIPAA's Administrative Simplification¹ rules and related matters for three reasons. First HIPAA mandates the adoption of interoperable standards including transactions and codes, privacy and security. The former are basically interoperable messaging standards but the latter require a new layer of interoperability among internal and between external systems. Second, by its very scope and focus, HIPAA diverts and delays other standards as well as other HCIT initiatives. In turn this will disrupt the HCIT market. Third, a lot is happening right now.

¹ For brevity, we will use HIPAA to mean its Administrative Simplification sections.

HIPAA at HIMSS

Although HIMSS 2001 seems a distant memory, it is a good place to begin this analysis. In fact, it was in the week prior to HIMSS that HHS announced that it was seeking clarification as to whether the HIPAA privacy rules were covered by President Bush's executive order to hold for review all pending federal rules. HIMSS was ready to explain HIPAA but HIPAA was slipping into play.

The HIMSS Leadership Survey found that HIPAA was the largest issue facing the industry. A year ago, recovering from Y2K projects of date certain, HIPAA seemed a distant, vague set of proposed regulations. In the intervening 10 months two of five major rules were finalized: transactions and codes in August and privacy in December. Two-year clocks were running. To this point most HIPAA efforts have been educational and internal, ironically often associated with risk analysis, which is part of the security rules that are not yet published. There is little enthusiasm among HCIT industry customers, the "covered parties" to jump into expensive HIPAA projects.

Educational sessions at HIMSS focused on explaining the new privacy regulation. Speakers noted that the final regulation added and changed many elements of the NPRM. Many other sources are available for the specifics so we will not review them here. Several speakers alluded to the frequent use of the terms "reasonable" and "appropriate" as modifiers softening what HHS was actually requiring.²

Rationalists, as exemplified by John Glaser at Partners Health, tried to put HIPAA in context. He maintained that hospitals already have a security framework in place. *Partners Health already takes measures to protect patients' privacy. It is part of good business practice and is based on reasonable industry norms. While it is unlikely that Partners could meet all of the requirements of privacy and security regulations, it has a good start. Thus Partners will not require new systems and crash projects to come into compliance when final rules are established.* In fact all hospitals and other covered parties do have some security and privacy policies and procedures in place.³ This is the position that HHS wants covered parties to take. Delaying publication of the final security regulations is not such a big deal now that one knows what the privacy requirements are.

Without commenting on how well Partners Health reflects the healthcare industry, such a moderate position belies the purpose of regulation.⁴ If all healthcare organizations' individual assessment of privacy and security needs were "reasonable" and sufficient, we would not need regulation. It is precisely because each organization's assessment may be different and some, in the view of regulators or standards bodies, inadequate that there are minimum requirements that all covered parties will have to meet.

Bill Braithwaite, HHS's senior advisor on health information policy, appeared at several venues. His basic message was that *HIPAA was here, why are you surprised because this is what you asked for; let's get on with it.* It is certainly understandable after the amount of work and effort invested in HIPAA by an under funded HHS and by interested standards groups and lobbies, that its architects were sensitive to a rising storm of criticism. After all, Administrative Simplification did evolve from [WEDI](#) proposals to save significant healthcare dollars by standardizing administrative and financial electronic transactions. Part of the deal between "the healthcare

² Based on Word's find function, the final privacy regulation uses "reasonable" 249 times, "unreasonable" 16 times and "appropriate" 365 times. If this is a useful analysis, one can note that HHS used the word "must" 952 times.

³ Another industry expert opined that it is a mistake to compare HIPAA to Y2K. This is correct but not in the manner expressed. Y2K had a specific problem potentially touching all systems and a date certain. HIPAA has undefined problems touching all systems with uncertain dates.

⁴ Partners Health's information systems, under CIO John Glaser's leadership, are recognized to be one of the top HCIT sites in the country. If they were in trouble, what would it say of the rest of the industry's chance to comply with HIPAA?

industry” and Congress was that in return for mandated standards that the public’s privacy would have to be protected – this requires security rules.

But this puts a spin on some regulation creep and HHS scope decisions that have sharpened a growing chasm between regulators and regulated. After all WEDI primarily represented those whose business interests were managed care transactions, the payers, not healthcare providers or others in the industry. Moreover, there certainly was no debate in 1996 on the scope and reach of the privacy and security regulations and their subsequent costs, particularly for providers.⁵

The rumors were stronger than the reassuring presentations that everything was on track. HIPAA was in trouble within the new administration, which was listening to powerful disgruntled constituencies including the AHA, the AMA and the pharmaceutical industry.

For the HCIT industry, HIPAA is discontinuous change. As pointed out in the last issue of *Standards Insight*, some HCIT vendors with large installed bases and some consultants may see their business increase with HIPAA. But HIPAA will consume the discretionary IT budget of hospitals and other providers. New projects will be deferred. Clinical systems’ initiatives, at the core of addressing IOM medical error findings, will be squeezed out to insure existing systems are “HIPAA compliant”.⁶

If HIPAA only diverted IT spending for a while, the HCIT industry would adjust. The real problem is that HIPAA is causing confusion and uncertainty among the customer base. This is a far more serious challenge to the industry because uncertainty causes buyers to delay decisions. The only way a vendor can make a sale is by taking on the risk of that uncertainty. Thus one heard the commitment by many vendors at HIMSS that they would insure that their products were “HIPAA compliant”. This is doubly dangerous. First as we will discuss next in the HIPAA section, HIPAA rules are likely to require extensive change. Second, the HCIT industry is selling product now while incurring future services liability – an almost certain recipe for future losses.

One side note from HIMSS, HL7 and Integrating the Healthcare Enterprise (IHE) each conducted interoperability demonstrations on the exhibit floor. Casual observation leads to the following. HL7’s small booth and theatre presentations were very crowded. IHE’s very large theater and demo areas were sparsely populated. IHE is a losing proposition. DICOM must be integrated into HL7 but IHE has nothing to offer beyond demonstrating imaging department workflow interoperability. There brute force method of developing profiles for all vendors and messages is not a model that can be extended to the rest of HCIT. If RSNA and HIMSS can continue to twist the arms of PACS and RIS vendors IHE will survive another year – but like the rest of the HCIT industry it is fighting for relevance in an increasingly preoccupied industry.

⁵ This might be an excellent learning experience for “industry” and who is reported to be speaking for them, particularly in an era of activist use of regulations to establish standards. This should be kept in mind as the NCVHS goes forward with developing recommendations for standards for personal healthcare record elements. There is great interest in mining clinical data by all types of researchers. The costs of getting that data at the source will not be born by those with vested interest in data standards.

⁶ We use HIPAA compliant loosely. It is the covered party, provider, plan or clearinghouse that must be compliant. In order to be compliant they must perform a risk assessment and a cost-benefit analysis and then adopt policy and procedures to implement the results of these analyses. Among such policy and procedure should be administrative and technical requirements. In turn the covered party’s information system must be capable of supporting such requirements. For example, the final privacy regulations specify that a covered party can use role base security to assure minimum necessary disclosure within its normal operations. Thus the information system must be capable of providing role-based security. In turn this assumes some level of access control. The information system must provide this. Of course, the information system is composed of many applications from multiple vendors, all of which must interoperate to provide these services.

HIPAA Administrative Simplification

HHS announced officially on February 23rd that the HIPAA privacy regulation's effective date had been delayed until April 14, 2001 to allow for a required 60-day period for Congressional oversight somehow missed by the Clinton administration on its way out of town. Concurrently the new secretary of HHS reopened a public comment period for 30 day ending March 30. Though one outcome of all of this could be that the existing privacy regulation goes into effect in April to be implemented no later than April 14, 2003, this is now an unlikely scenario.⁷

There is real opposition to the privacy regulations (and presumably to the yet to be finalized security) regulations. Some of this opposition is seeking to kill the onerous terms, some to fix them and some to seek payment for implementing them. However, once a forum is opened, uncertainty reigns and in fact may spread to other areas, even the standard transactions. This is brief discussion of the major points of contention

Costs of Compliance

Covered parties, particularly providers, incur significant, unreimbursed costs. HHS estimates that the ten-year cost of complying with the privacy regulation will be \$17.6 billion (or \$11.8 when discounted to net present value). That is 2.5 times the estimated total costs of implementing all of the rest of Administrative Simplification (including security). There is obviously something wrong with these estimates. It is primarily in how HHS has avoided including the costs of the security regulation. In the security NPRM two rationales were given for not providing a separate cost estimate in the Impact Analysis. First, security was just a cost of doing business and thus would not add incremental costs to covered parties. Secondly, to the extent there were costs they were aggregated in the overall cost estimates prepared by the actuaries and published first with the national provider identifier NPRM. Going to this source, one finds that the estimated costs of implementing administrative simplification, i.e., \$7 billion, over 5 years, is really derived from WEDI cost estimates for implementing standard EDI transactions. If ever formally considered, security was viewed as a small add-on to messages not the comprehensive regulation of entire organizations that it became in its NPRM. Mechanically even the \$7 billion is understated since it is the cost to covered parties pro-rated by whether they would prepare electronic transactions themselves compared to those that would use clearinghouses or only paper claims. Practically all healthcare providers will be covered even when they turn over paper forms to a billing service or clearinghouse.

The American Hospital Association is seeking reimbursement for implementing the regulations. Most costs to providers will occur in the first few years during implementation. For example based on HHS estimates for all of Administrative Simplification, except privacy, and for privacy, 54 percent of the ten-year costs will be incurred in the first three years.⁸ These cost estimates are obviously flawed. The failure to include any meaningful costs for implementing security regulations across an entire organization strengthens the alternative estimates that show HIPAA to be a far more expensive undertaking with much less payback.

Moreover the AHA's position seeking reimbursement is even more powerful when one considers that hospitals will not benefit from the "savings" for which they are investing. We, the people, and our payer-surrogates save. Who believes that Medicare or managed care plans will allow providers to keep future savings in the form of pass-throughs and higher margins? This is not bad on balance, but it is the essence of unfunded mandates. This will be a recurring theme when we get to a next generation of regulatory standards. Unfunded mandates will also be a primary lobbying target by AHA as a more politically tuned means of increasing reimbursement.

⁷ The last public comment period on privacy produced more than 90,000 responses. HHS will need more than the two-week interval between the close of comments to the effective date to read, even without considering, the expected number of responses.

⁸ However, HHS estimates that all costs of Administrative Simplification, minus privacy, will disappear after the third year.

HIPAA does not pre-empt state and other federal laws.

Many had hoped HIPAA would reduce the complexity of different state privacy laws. For multi-state covered parties and for the HCIT industry it would be very beneficial to be able to operate under a single privacy and security regulation, not under both it and individual state laws. Moreover, the issue of whether a law is more or less permissive is really secondary to whether it is different. Many states, not only have their own laws, but are developing new privacy laws.

Without all the final regulations published, it will be difficult and wasteful to implement them in a piecemeal fashion.

The sequential release of final regulations will cause wasted effort, rework, and interim solutions. Without the security regulations, privacy is difficult to implement. Security is the real key to moving forward with implementation. To some extent, large organizations can partition the electronic transactions at the outer bounds of their system. Translations, mappings and extractions to support the standards can be done independent of the security that will be wrapped around the message when it is actually sent. However, this represents a small portion of the changes and costs that Administrative Simplification imposes. Privacy and security apply across the entire organization and to business associates. Some of the privacy rules, such as obtaining and tracking consents, authorizations and disclosures, can be implemented, as they exist now. Of course this implementation will depend on paper forms and manual signatures since the electronic signature rules are not yet published. Many of the privacy policies, such as for minimum necessary disclosure, could be developed now. But they cannot be implemented yet unless one is willing to guess what the security regulations will say. For example, role-based security is a means of implementing a routine minimum necessary disclosure policy. Role based security implementation would involve decisions about access control (identification, authentication, authorization). Yet minimum necessary is not the only source of access control requirements. For example the security regulations themselves set up requirements to insure data integrity and availability, interrelated to access control but independent of the privacy rules. The point is that the security rules are the foundation for implementing privacy requirements. Piecemeal implementation of security applications is unlikely to result in either a secure or cost effective system. It is contrary to the plan initially laid out by HHS to enable system upgrades and modifications to be made as part of a comprehensive play to minimize do-overs, crosswalks and interim solutions.

The two-year time frame is challenged.

HHS acknowledges frequently in the regulations that it really does not know what it will take to actually implement the regulations because nothing of this scale has been done before, not in healthcare, not anywhere. Moreover, even for the most straightforward rules, those covering the standard transactions, [SNIP](#) is finding many small and not so small problems in trial implementations of just the 837 claims transaction. These include problems with codes, with use cases and workflow, and with missing or unavailable data. For example, there are a number of technical issues to resolve and fix for both the transactions and privacy rules to work together. These could be done as modifications to the existing rule but are also evidence of the need for deeper change. These include things like establishing retail pharmacists as direct care providers, subjecting them to consent and authorization requirements. In theory, a pharmacist must obtain a signed consent from the patient prior to acting on prescription. Further a family member would not be allowed to pick up a prescription without a signed authorization by the patient. There are similar concerns about scheduling new patients and obtaining eligibility data before a consent form is obtained.

These problems have not been fixed despite fast track mechanisms within the designated standards maintenance organizations (DSMOs) that recommend to NCVHS and then to the secretary. SNIP has not yet begun to focus on the other seven transactions, and 25 percent of the total time to implement, test and put into production all of the transactions has elapsed. If this is the simple side of Administrative Simplification, what happens when covered parties start to implement privacy and then security?

The tension for HHS in granting any delay is twofold: it takes the pressure off those who are hard at work and it strengthens those seeking to radically change or kill the rules.

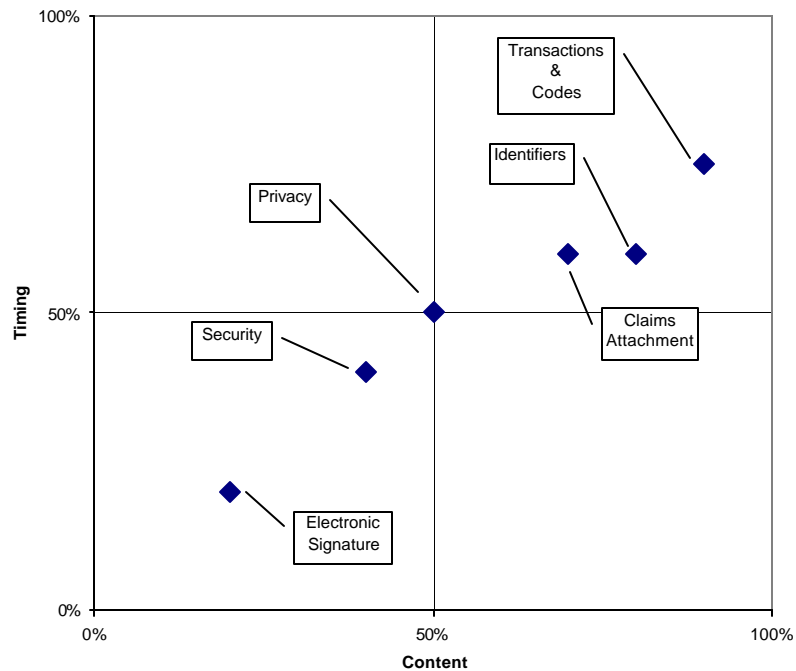
Digital signature

As discussed in the previous *Standards Insight*, electronic signature remains a pivotal rule, which is still unlikely to be part of the final security regulation. In its recent meeting the ANSI HHSB (Health Informatics Standards Board) decided to formally take over coordination efforts such as the one started by the multiple standards development organizations. It is based on the clear recognition of all parties that there are multiple uses of digital signature including as an electronic signature and as a data security mechanism and that there is a need to consider an interoperable public key infrastructure to manage certificates. The coordination was divided into two scopes: use of electronic/digital signature and the public key infrastructure (PKI). The [multi-SDO group](#), now under ANSI HHSB, continued with their action plan. They will focus on the use of electronic/digital signature in documents and messages. They expect to have a scope statement and plan by the end of March. A joint effort between Tunitas Group and the [Medical Records Institute](#) will take on the PKI issue. Specifically they will seek to evaluate costs and benefits of eSignature in healthcare. This is a difficult economic issue. Any organization can establish a secure, digital signature environment internally. The problem becomes one of interoperating among other organizations and in funding the external authorities necessary for such interoperability. The joint group is target preliminary results by May's TEPR meeting. Although HHS may continue to defer final rules for electronic signatures, it is a security technology interoperability issue that could slow down implementations. One cannot go back and make data and documents more authentic or more secure after the fact. Moreover, the technology and infrastructure cost issues may not be ripe for regulation.

HIPAA Outlook

HIPAA scenarios can be described on two axes: content and timing. Both are interrelated and both are in play. Figure 1 shows our estimate of the certainty of current content or expected implementation date based on the preceding discussion. Timing, or delaying implementation

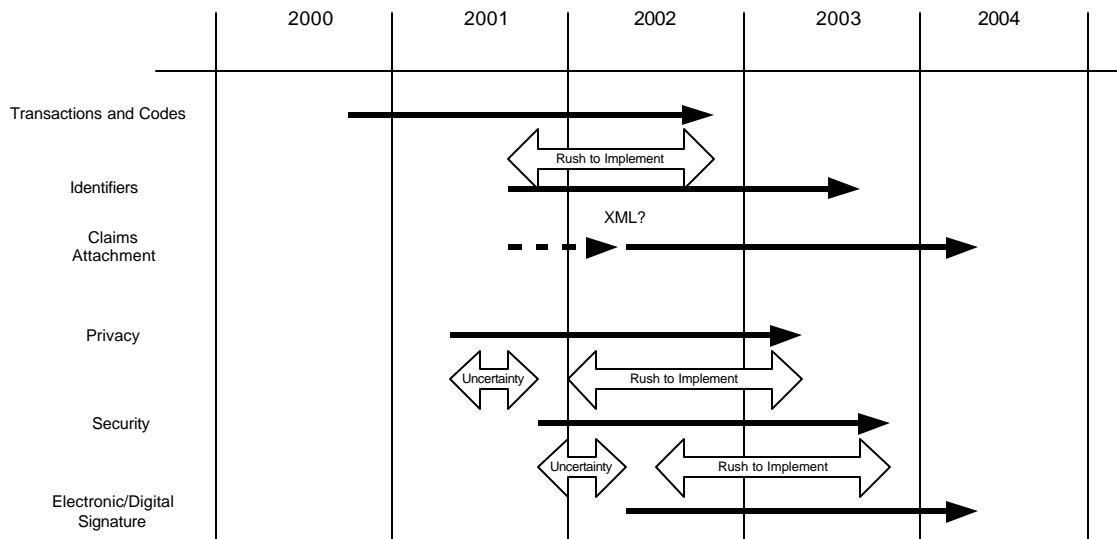
Figure 1. Positioning the HIPAA Rules



dates, is the easiest parameter to manipulate. Extending deadlines also provides the opportunity to change and fix content. Uncertain content obviously contributes to uncertain timing.

In general, the financial rules associated with standard transactions are most probable. The biggest issue is timing and we will discuss it below. Privacy is a fifty-fifty proposition. However, if we take the current and expected dates for all the major provisions of Administrative Simplification, we can plot out a timeline. Figure 2.

Figure 2. Current HIPAA Implementation Schedule



We highlight several gaps caused by the publication of interrelated rules at different times. Such gaps first cause uncertainty in implementing the first published rule, e.g., transactions and codes and privacy, until related rules are published, e.g., identifiers and security. This front-end gap reduces the amount of time left to implement the first rule, causing a more accelerated and costly implementation.

What changes to the privacy rule, if any, might we expect:

No Change

HHS sticks to its April date for privacy and uses the first year to modify. HHS then publishes the final security rule by end of fiscal year. Security has no significant changes except for conformance with privacy. This is an increasingly unlikely scenario. Secretary Thompson, as a former governor, is unlikely to allow such massive, unfunded regulations to be added to healthcare without real management review.

Alignment of Privacy and Security Dates

HHS decides to use the next 6 – 12 months to consider public comment and fix privacy. Then it will time align privacy with security. This reduces the uncertainty/rush to implement gaps. Thompson decides to get the funding and conduct a full review openly and effectively. It is becoming the more likely scenario. It may still leave the electronic signature rule unresolved.

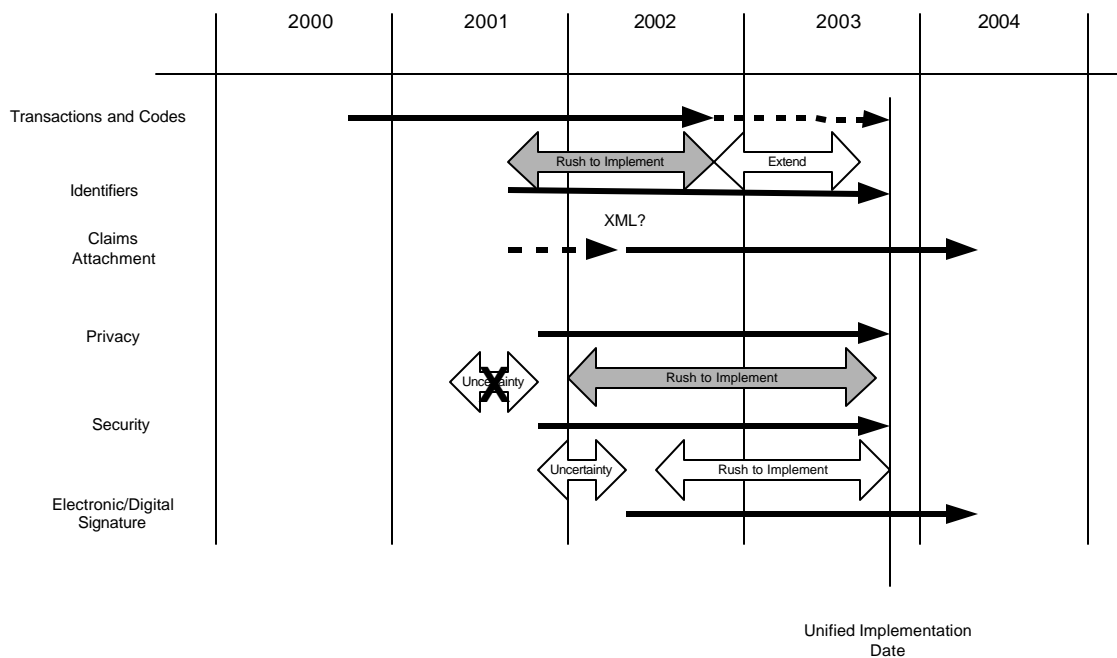
Major revision

Although the new administration is probably not anxious to spend the time and energy going back and fixing the mess of the last Congress and administration, it is possible that the new secretary will conclude major changes are needed or that such far reaching regulations are not good for the industry or for patients. In fact the more thorough the

review in the previous scenario, the more likely it becomes that significant change occurs. Congress may be forced to address the unfunded mandate issue and rethink privacy in a broader context. This is unlikely now but will increase in probability over time.

Figure 3, shows how one could align all the implementation dates sometime after the end of fiscal year 2003. This solves a number of issues including requests to give the industry more time to implement standard transactions. WEDI, after holding public hearings and getting consistent feedback, is recommending that the implementation date for privacy not become effective until security is available.⁹ Likewise they are seeking delays in assessing penalties for missing the transactions date. This is likely to become the broad consensus position and be the path taken by HHS. The biggest question is not whether such alignment will happen, but given a real review, when will the date occur.

Figure 3. Probable Changes to HIPAA Implementation Schedule



Outlook for HCIT Industry

This delay and reopening by a new administration is more likely to result in change and anticipated change creates uncertainty. Under any of the scenarios the HCIT industry is looking at uncertainty, probably throughout 2001. These delays and implementation alignments allow our customers to better plan and implement the rules, but we still start out with the initial period of uncertainty without final rules. Until customers understand the standards to which they will be held, they will refrain from making new application and system commitments. While one might say that the security and privacy rules are not primarily about technology, they touch every system. Every system and its data must be analyzed in terms of its security risks. Based on the overall cost-benefit analysis of the healthcare organization and its determination of what it will do to insure the security and privacy of personal health information, each system will need to be

⁹ They recommend a similar date alignment for transactions, codes and the not yet final rules for employers and providers identifiers. This would also result in delaying the transactions and codes implementation date to April 2003 from October 2002. In fact WEDI recommends that HHS extend the enforcement date for transaction to October 2003.

brought into compliance with the healthcare organization's technical framework. Does anyone know what that means yet? What CIO would want to make decisions on system security without knowing what those minimums are, particularly when these types of regulations have never been implemented before? Moreover, what CIO would want to make their decisions before they knew what their vendors would be able to offer and at what price?

Bottom line

The privacy regulations and the security NPRM represent regulatory overreach. Had Congress met its responsibilities and had HHS decided to limit its scope to insuring that the standard EDI transactions and the data they contained were kept private and secure, we would probably be well into gaining the expected benefits of Administrative Simplification, perhaps within the cost estimates. However, by expanding the scope to an all-encompassing security regulation and an expansive, but not all-inclusive¹⁰, privacy regulation, we are potentially left with untried regulations being applied to one seventh of the economy in a two year window. The new administration faces some difficult choices. It says it wants to tackle Medicare reform but may have to tackle HIPAA first. The law of unintended consequences begins to apply. The federal government in its attempt to speed up the adoption of uniform standards will actually delay them more than if the market had been left to solve the problems. Moreover, by always looming on the horizon, HIPAA privacy and security regulations insure that no alternative options are widely implemented.

Right now HIPAA will delay and redirect spending on HCIT. Of the two, delay will be the most harmful to HCIT. Until customers understand the standards to which they will be held, they will refrain from making system commitments.

Next Issue

The next issue of *Standards Insight* is planned for the end of May. It will attempt to catch up on other standards issues, including the diverse efforts to standardize medical records and quality data. Undoubtedly there will be some updating of HIPAA related standards, such as digital signature and security.

Comments or questions about *Standards Insight* may be directed to [Carla Smith](#) at CHIM or its author [Ed Larsen](#) at E. R. Larsen, Inc.

¹⁰ The privacy regulations only apply personal health information maintained by the covered parties and their business associates. The more general issue of PHI and consumer privacy is yet to be addressed by Congress and, as noted, the subject of many and different state laws.