It's 2002: How HIPAA-ready Are You?

By Kevin J. Wilson and Clint E. McPherson

HIPAA, its implications for how healthcare organizations (HCOs) do business, and opportunities it may offer for increased automation and process improvement are hot topics. While some HCOs have completed their HIPAA assessments and are implementing needed changes for compliance, many others have not yet begun. Time is running short.

The HIPAA transactions standards are not just technical issues; the data content from the business users must be present to fulfill the requirements. The privacy requirements are manageable if their impact on the organization is understood in detail. The security standards loom on the horizon and present challenges to healthcare IT managers. It is time to face the project head on and institute business changes to comply with the regulations.

Transaction Standards

In the next few months, organizations should develop strategies for complying with the electronic transactions standards. The reason for this is twofold:

1. These transactions are the key to cost savings and business efficiency because they provide pathways for automating and standardizing existing key business processes, such as patient access and back office processes;
2. Non-compliance with the HIPAA transaction standards could result in a substantial increase in denied payments and/or lost revenue.

Organizations that utilize third party vendor applications rely heavily on vendors to provide necessary HIPAA "patches" within their applications. This reliance is justified and should be pursued. But understand that a significant amount of work may be required to interface these applications with one another. How much depends upon the level of customization to third party applications within their respective environments, and the variety of applications utilized by the HCO to capture patient health and/or billing information.

> Organizations should have drafted their Notice of Privacy Practices and should be making plans to address consumers' questions and requests to exercise rights.

In addition, some of the required and/or situational data elements being addressed by the HIPAA transaction standards are new or have not been utilized in the past. Changes to business processes and procedures may be required to ensure accurate information is captured and provided for HIPAA transaction(s).

One example of process change would be an organization's efforts to update the physician master file with taxonomy codes. Most likely, responsibility for updating the physician master file with appropriate codes for current physicians, as well as determining appropriate codes for physicians who request privileges in the future, will rest with the physician services/credentialing department.

Another example of a business process change that may be required is in the area(s) responsible for charge description master (CDM) updates. Under the NEDI Transaction Set Implementation Guide (www.wpc-edi.com), organizations submitting an 837 claims transaction that are also conducting research must include the FDA investigational device number as a data element within the transaction. Assuming the organization utilizes the CDM to ensure the FDA number is passed to the transaction, those conducting research will need to closely coordinate with the person(s) responsible for CDM updates to ensure charges associated with research utilize the correct CDM charge and FDA number(s).

By now, healthcare organizations should have evaluated the NEDI Transaction Set Implementation Guide to determine business and/or technical areas requiring changes, along with the level of change required for these areas. To streamline this process, organizations should work with their third party vendor to obtain a data element crosswalk between HIPAA transactions and their current systems layout. Understanding these changes will help ensure customized fields are not used in place of the vendor supplied fields. This crosswalk will also be important in identifying where vendor system updates may occur to help

the business better understand changes that may be required to complete the data elements portion of the transactions, along with the future training needs created by the changes.

Organizations with systems developed in-house should be in the remediation programming phase of their project. The field additions and screen changes that may be necessary to capture HIPAA data elements could be substantial. Organizations that didn't start remediation by the end of 2001 may need to consider outsourcing or co-sourcing the programming changes or implementing a new third party vendor system to meet the HIPAA transaction standards compliance deadline of October 16, 2002.

Privacy

It's January 2002. Organizations should have completed their HIPAA privacy assessments, have a detailed understanding of how the privacy rules affect their operations, and have a plan to implement those changes throughout the organization. From a business perspective, the most demanding components of the privacy requirements include the Notice of Privacy Practices, Request for Restrictions, Business Associate Agreements, and Minimum Necessary.

While each area presents its own organizational challenges, it is important for organizations to keep the "reasonableness" criteria in mind when planning organizational changes. The latitude provided by the use of this term gives organizations the ability to approach compliance in ways that make good professional, business and financial sense for the organization.

The Notice of Privacy Practices, while not a significant burden to draft, becomes an organizational challenge to implement when published. While many of the patient rights provided under HIPAA already exist in some states, patients may not be aware of them. The mandate to publish a Notice of Privacy Practices almost guarantees there will be questions and requests. Some patients will query prior to signing the consent to use health information; others will wait until they are in the waiting room and have an opportunity to read the document. As a result, there are sure to be questions and requests from individuals to exercise these rights.

> HIPAA *does* offer HCOs the opportunity to integrate HIPAA compliance efforts into other ongoing strategic initiatives.

Some organizations have established centralized offices to address patient requests; others will utilize existing services such as patient relations, medical records, compliance, and/or risk management to address them. Either way, organizations should have drafted their Notice of Privacy Practices and should be making plans to address consumers' questions and requests to exercise rights.

The Request for Restrictions requirements state that the restriction must be documented but do not give a specific timeframe in which the decision to accommodate or reject the request must be made. In accordance with sound business practices, the request should be reviewed and a decision made within a reasonable period of time.

The decision to accept or reject a request for restriction should not be entered into lightly by HCOs. These restrictions, once agreed upon by the organization, become legally binding. Some organizations have decided to address requests through a committee format, while others have placed responsibility with a particular department. The critical component, given the effective date of April 14, 2003, is that organizations make a decision on how requests will be addressed and prepare to train the organization in recognizing such requests and forwarding them to the appropriate personnel.

By the beginning of 2002, organizations should have identified the responsible committee or department and should be working with these individuals to establish an efficient business process and assist in understanding the organizational issues in accepting unreasonable requests.

The Business Associate Agreement portion of the requirements has had a significant impact on organizations that have completed the assessment phase of a project. Many have found that they have outside agencies working within their facilities, with access to health information, that are not bound by a formal contractual agreement. These organizations are working to inventory all such relationships to develop or amend contracts with them by the end of 2002.

Many organizations lack the available in-house legal resources to review these relationships to properly address the contents of a contract within the desired timeframes. Also, many organizations are considering outsourcing the legal review of these contracts to ensure adequate time for any business process changes necessary with an April 2003 deadline.

Numerous HCOs are having difficulty addressing the Minimum Necessary components directed at employee access to health information, because compliance may involve information gathering and information systems access changes.

Continued on page 20

Organizations should be in the process of classifying personnel and health information into roles, groups or classes. Logical security classifications should be tested and retested prior to finalization to ensure they do not increase the risk of non-compliance or too strictly limit access to health information such that business functions are impaired. Organizations should complete this part of their HIPAA project as soon as possible; this information is necessary to assist in development/refinement of access to information systems for HIPAA security rules.

Security

HIPAA security regulations are not finalized—so why address these areas now? HIPAA security regulations are a reflection of security best practices, and the privacy requirements have a requirement that technical and physical controls be in place to safeguard health information.

Because of the safeguards requirement, many organizations are addressing the security requirements with the privacy requirements, and some organizations are addressing the security rules as the mechanism to enforce the privacy requirements. Regardless of approach, right now HCOs should be evaluating their environment and beginning the planning and budgeting process for system changes to enforce the security components of the regulations.

Integration and Completion

HIPAA *does* offer HCOs the opportunity to integrate HIPAA compliance efforts into other ongoing strategic initiatives. For example, one organization that wanted to re-evaluate its registration/admissions function included a HIPAA assessment in the process. Now, as they redesign business processes and establish registration metrics, they take into consideration the HIPAA eligibility and authorization transactions to ensure these requirements are designed in as part of their process realignment efforts.

Other organizations have included the transactions and security components into their IS update/implementation projects, which maximizes programming cost efficiencies and opportunities to automate or redesign business process. By incorporating HIPAA into existing projects, these organizations take better strategic advantage of HIPAA and should be prepared by the regulations' effective dates.

> Organizations that utilize third party vendor applications rely heavily on vendors to provide necessary HIPAA "patches" within their applications. This reliance is justified and should be pursued.

In summary, some HCOs have completed their HIPAA assessments, while others wait on the sidelines, hoping it will go away. But it's not going away, and compliance dates are closing in.

The transactions standards represent revenue and net income to healthcare organizations and are significant. HCOs should be testing HIPAA transactions with their business partners by no later than the end of the second quarter, 2002. Once this process is complete, some resources may be redirected to the privacy components for the duration of 2002. Organizations should have their business processes designed to address these rules by the end of the first quarter, 2002. These processes will require substantial policy and procedural drafting and education for the entire enterprise. This process may take the remainder of the year, with a goal of completion by first quarter, 2003.

Ideally the security portion of the rule should be integrated into the privacy compliance efforts. If they are being addressed independently, organizations should conduct an assessment in the first quarter, 2002. Plans for system changes can then be developed through second quarter, allowing for deployment in third and fourth quarters. This would align with the organizational privacy training efforts and could be utilized to educate the organization on security changes planned to support privacy requirements.

While HIPAA poses a number of challenges for healthcare organizations, it will be a pivotal opportunity for many HCOs to strategically transform the way they do business and align their overall business strategies with the requirements of HIPAA, while increasing their return and long-term operational benefits from this process.

Kevin J. Wilson is project manager at Arthur Andersen LLP, Dallas. Contact him at kevin.j.wilson@us.arthurandersen.com.

Clint E. McPherson is a senior manager at Arthur Andersen LLP, Dallas. Contact him at clint.e.mcpherson@us.arthurandersen.com.

HMT