Countdown to Compliance: Privacy

by Sybil Ingram-Muhammad, MT(ASCP), PhD

How far along the road to compliance with the HIPAA privacy regulation is your organization? This article tells you the steps you should be taking to get in compliance by the April 2003 deadline.

It is February 2002—14 months before your organization has to be compliant with the HIPAA privacy regulation. Part of the 24-month time frame for implementation has expired and cannot be recaptured. How ready would you be *today* to confront and address allegations of a privacy breach that occurred in your covered entity? Let's back up a minute. Would you know that the breach had occurred *before* you received the call that you would soon be paid a visit by the Office of Civil Rights because of such an allegation? This article offers a quick summary of many of the important things you and your organization should be doing to ensure you will be compliant in time.

The HIPAA Privacy Regulation of Title II, Subtitle F, a portion of the larger Health Insurance Portability and Accountability Act, was adopted as a final rule on April 14, 2001. The myth that a covered entity does not have to do anything about coming into compliance with this rule until April 14, 2003, has the type A proactive personalities struggling with the consummate procrastinators very much like the Hatfields and the McCoys.

Adoption of the rule means you can start working now to fulfill the expectations in the rule; the time frame for compliance sets the expectation that a plan will be put in place and working—before you begin to entertain unexpected phone calls and potentially uninvited visitors. With 14 months left to go, have you started HIPAA remediation activities within your organization, or have you succumbed to the "analysis paralysis" syndrome, in which you are not doing anything because you are still figuring out what to do?

For the sake of discussion, let's assume that at least the following things have occurred at your organization:

• You have heard about HIPAA, learned that it has a privacy component, and by now come to realize that, tag—you're it! You are some type of covered entity as defined by HIPAA and you have to *do* something about this regulation.
• You have probably taken more than a glance at the regulation and realize that there is quite a bit being said here, as well as quite a bit to do—soon.
• You have intelligently deduced and consciously made a decision that it would probably be in the best interest of the organization or entity to assess where you currently stand against the requirements to better position yourself for making future intelligent and informed decisions regarding your remediation efforts.

Assessment: Where You Are, Where You Will Be

Performing an assessment of where your organization stands today against where your organization needs to be is the critical first step every organization needs to take toward developing a compliance strategy. Never has the phrase "due diligence" meant more than it means now with regard to your compliance initiative and willful intent to "do the right thing." An assessment of your organization is demonstrable evidence of such diligence. The assessment may be performed by members within the organization or by an experienced third party, but an assessment must be made.

You can't (or shouldn't) proceed with implementation until your organization has made some crucial decisions based on this assessment. Once the assessment has been completed and the results have been communicated to the executive management of the organization (no matter if you work for a covered entity organization of one or 1,000) and understood by them, the covered entity will need to determine its level of risk tolerance. How risk accepting or risk averse a covered entity is should be the initial and primary driver for making compliance direction decisions and setting plans, goals, and tasks. This decision needs

to be made by executive management, who will ultimately be held accountable for the effectiveness of the organization's compliance or lack thereof.

As HIPAA itself is an unfunded mandate, your privacy initiative requires funding to be successful. Cost estimates for budgeting purposes for this initiative should be addressed during the assessment. Again, the organization's level of risk should be determined before the first dollar is spent on any remediation activities. Although not all compliance requirements under the privacy regulation will require capitalization, inadequate funding for this portion of your overall HIPAA compliance strategy may result in unnecessary setbacks, rework, avoidable failures, and potential overexpenditure of resources in terms of personnel time and expenses.

Another important step is to determine what the term "reasonable" means to your organization. This is an important consideration and driver that will require substantive deliberation on the part of executive management and all personnel responsible for the execution of organizational privacy compliance.

The privacy regulation uses "reasonable," or some variation of this word, more than 250 times. The subjective nature of the word has caused consternation across the industry; what is considered reasonable by one entity may not be considered reasonable by another. Although this issue is one of the most challenging aspects of meeting the expectations of this regulation and is the subject of tremendous philosophical debate and interpretation, analyzing and defining what is going to be considered reasonable cannot paralyze the covered entity's individual compliance initiative. We must get on with the work at hand as time to compliance continues to contract.

Who's On First: The Privacy Officer

Per 164.530(a)(1)(i), the covered entity must designate a privacy "official" or "officer." This person will be responsible for the development and implementation of policies and procedures related to privacy. He or she will need not only the responsibility to execute these expectations but the authority as well. The privacy officer does not have to be new to your organization—in fact, many HIM professionals are stepping up to the role.

Although the privacy officer may have the responsibility for developing and implementing policies and procedures, he or she does not have to do this alone, nor should be expected to. To succeed, the privacy officer needs a dedicated team (for example, a HIPAA privacy task force) with representatives of all departments or personnel within the covered entity. Ideally, someone will volunteer freely from each department; be mindful of the fact that you may need to "implement a draft" as the importance of this legislation may not be innately apparent to everyone.

One area that must be represented on the task force is general counsel or the legal personnel of the covered entity. Creation or modification and execution of HIPAA-compliant business associate contracts that include required verbiage (160.504[e][2]), comparison between the state and HIPAA privacy requirements with regard to preemption (160.202), and identification and documentation of the HIPAA-defined healthcare operations of a covered entity are just a few of the tasks where legal expertise will be essential. Some of these tasks may be outsourced to an experienced healthcare law firm that has a HIPAA specialty component, but to be of value such a firm will need the input of operational knowledge from a representative of the covered entity. Of course, the best source to contribute to this process is someone with credible, integral knowledge of the organization.

The privacy officer and the task force must necessarily become the organizational experts on the privacy regulation. (See "What You Need to Know" for a list of important concepts to know.) With this in mind, a portion of the funding for this initiative must be identified and dedicated to initial and ongoing education for the privacy officer and the task force. Many avenues for initial and continuing education should be explored to meet this need (on-site training, Web sites, computer-based training tutorials, conferences), but a commitment to the task force's education will ensure a more desirable outcome of their efforts. Subject matter expertise on various portions of the regulation should be encouraged and divided among the task force members under the guidance of the privacy officer.

Building the To-Do List

Next, a plan must be developed and should be approached much like any major project. Make sure to include:

• goals
• tasks
• resources
• deliverables
• dates of initiation and completion
• predecessors
• dependencies identified and assigned

The plan will need to include change management methodologies and clear communication pathways. It will need to be flexible and dynamic so that modifications to the rules and regulations during the implementation period can be incorporated into the plan as transparently as possible. (Modifications have been proposed and are expected; expect scope changes to your plan, and be prepared to address the dreaded "scope creep.")

Special attention and consideration are warranted where the security regulation and privacy regulation cross over with equal (as in training and documentation) or idealistically similar requirements (need to know versus minimum necessary). The equal or similar requirements should be identified and addressed as a part of the plan in an integrative manner with the HIPAA security task force to minimize redundancy and coordinate efforts where possible.

For example, the task force may decide to devote 60 percent of its time to policy and procedure development and documentation, plus required form development and documentation (consent forms, authorization forms, privacy notice development and posting). "Policies in Place?" below, lists some of the important policies and procedures to develop.

In this example, the remaining 40 percent of the task force's time might be being devoted to the development of HIPAA privacy training materials, delivery of actual training, and working with the entity's human resources department or designee to ensure that documentation of training is captured and placed in the staff's respective personnel files.
The words to live by here are "Educate, educate, educate, document, and be prepared to educate again." Here's where your organization's level of risk tolerance comes into play, as it is imperative that policies and procedures, corresponding forms, and training all reflect the level of risk decisions the organization is willing to accept *and defend*. Accordingly, these elements should not be developed until risk is addressed.

It is also advisable that the plan contain a mock compliance inspection or a mock sentinel event that will allow the organization to benchmark its organizational readiness, preparedness, and mitigation processes, if applicable, against the regulation. Monitoring and ongoing enforcement and reinforcement should mark the end of the remediation initiative and the commencement of an effective and efficient HIPAA privacy compliance program.

There's a lot to do to implement the HIPAA regulations. In a sense, there's just as much to discuss and decide as there is to do. That's why it's important to begin now—if you haven't already—to move toward compliance. HIM professionals are certain to be at the center of this work in the coming months, so it's critical to be proactive and keep the process moving on schedule. u

Sybil Ingram-Muhammad *(smuhammad@beaconpartners. com) is engagement manager, enterprise security and HIPAA compliance, at Beacon Partners, Inc.*

Policies in Place?

Developing policies and procedures related to privacy is a major challenge. Some policies and procedures that need to be developed are:

- **consents**—delineate when required and when not required
- **authorizations**—when required and when not required
- **amendment** of the designated record set by a patient
- **access** to the designated record set by a patient
- **copying** of the designated record set by a patient
- **denial of access** or amendment or copying to the patient of the designated record set by the covered entity

- **nonretaliation** against whistleblowers
- **opt-out policies** regarding facility directories, receipt of marketing materials, and fund-raising activities
- **verification of identification** prior to the release of PHI
- **complaints** made to the covered entity for suspected breaches or infractions of PHI by patients or employees
- **sanctions** for privacy breaches or infractions
- **release of PHI** to clergy and law enforcement

ASample Timeline

With only 14 months left to go to implement the privacy regulation, every day counts. Here's a sample timeline for a fictional healthcare organization following the steps listed in this article.

February
privacy officer and task force appointed; begin risk assessment (assess organization's risk tolerance and estimate financial resources required to achieve compliance)

March
send letters to third parties asking for their progress with achieving HIPAA-enabling strategies for your organization. Get the response
in writing. Conduct state privacy law vs. HIPAA privacy standards comparison and analysis

April
present findings of assessment to senior management and HIPAA task force; senior management decides level of risk organization is willing to assume, financial resources allocated

May
review business partner agreements; identify new business associates to
replace uncooperative ones

June
identify, define, and document healthcare operations (HCO) for the organization

July
begin work on draft policies and forms

August
complete policies and procedures, forms, and HCO development;
submit and receive approval by senior management

September
design of training and materials begins

October
begin execution of business associate contracts (BACs)

November
training of staff, clinicians, and other employees begins

December
receive BACs from business associates

January
mock sentinel event to benchmark readiness; identify and correct deficiencies

Fe bruary
training activities finish

March
mock sentinel event #2 to benchmark readiness

April 14
compliance readiness achieved

What You Need to Know

An organization's privacy officer and privacy task force need more than a superficial knowledge of the privacy regulation. It will be critical for all to gain a better understanding of some of the following concepts:

- the differences between privacy and security
- consent and authorization
- use and disclosure
- direct and indirect provider
- affiliate versus hybrid entities
- protected health information (PHI) versus just individually identifiable information
- who is a business associate (for example, outsourced legal counsel, repricing services, third-party administrators) and who is not (for example, members of your work force), when a business contract is needed, and the covered entity's privacy and security expectations of the business associate
- what is required when a covered entity is conducting research using PHI versus conducting research that contains a treatment component
- the minimum necessary provision (164.502[b][1] and 160.514[d])
- when an organized healthcare association declaration would be appropriate and how to leverage the development and implementation of joint consents, authorizations, and privacy notices under an organized healthcare association
- when exceptions to most of the above apply, or where state law is more stringent than the rule (and therefore preempts it) or other special provisions related to state law or other regulations

Article citation:
Ingram-Muhammad, Sybil. "Countdown to Compliance: Privacy." *Journal of AHIMA* 73, no.2 (2002): 28-32.