On the Fast Track to Privacy Rule Compliance (HIPAA on the Job)

by Margret Amatayakul, RHIA, FHIMSS

Whether your privacy rule compliance efforts began two years ago or yesterday, you're probably concerned about the April 14, 2003, implementation date. In this article, we'll explore some of the ways you can make the most of the time remaining.

Don't Skip the Assessment

If your organization conducted a readiness assessment months ago, it may be sitting on the shelf while you're putting the finishing touches on policies and procedures, getting them approved, and preparing training materials. And if you haven't conducted such an assessment, you may be thinking of skipping it in favor of moving straight to remediation. However, in either case, the assessment is useful for the following four reasons:

- **An assessment does not need to be highly detailed, time-consuming, or expensive to be effective.** In fact, it could entail combining a staff exercise, self-assessment, and external validation. A self-assessment tool that provides sufficient direction can engage every component of the organization. Then an unbiased observer can use a sampling and benchmarking approach to highlight critical issues and offer best practice solutions.
- **An assessment identifies operational issues specific to your environment.** Whether you approach privacy rule compliance in a linear fashion or all at once (which a fast-track approach may require), you need to determine how the regulations fit into your facility's day-to-day operations, whether technical support is needed, what effect there will be on work flow, and how to change current attitudes about use and disclosures. Old policies and procedures may need to be revised or retired and old forms will need to be modified or discarded. An assessment provides the opportunity to achieve genuine operational compliance, rather than the appearance of compliance on paper.
- **An assessment helps prioritize tasks.** While you will ultimately need to address all HIPAA standards, there is a logical sequence appropriate for each organization. For example, some organizations have problems with incidental disclosures, so physical security and other safeguards may need to be the initial focus. Other organizations require patient rights education, so confidential communications, restrictions, amendment, and even access concepts may need greater attention than other issues. Complex organizations may need to first establish which components are covered entities and which must be designated affiliated covered entity status, covered components of a hybrid entity, or part of an organized healthcare arrangement. These issues are unique to each organization and cannot be fully understood from rote application of the regulations.
- **An assessment is a legal document subject to discovery in an investigation or lawsuit.** If a covered entity is found to have known about a gap, but did not take reasonable steps to overcome it, and a violation or a breach of confidentiality occurred, the assessment will play a critical role in identifying the entity's obligations. Don't consider this a reason to skip the assessment, because the fact that a covered entity "should have known" or "should have taken prudent steps to discover" could be used to support a case in the absence of an assessment. On the positive side, an assessment can support that appropriate practices and procedures were found to generally be followed and an action under scrutiny is an aberration.

Share the Responsibilities

The HIPAA privacy rule affects virtually every person in a covered entity. Those on the fast track may find that they do not have time for a project manager to lead committees to do the work for all. Instead, everyone will need to roll up their sleeves and become involved in implementing the requirements.

While a steering committee can be valuable, keep in mind that the individual members of the work force in the trenches are likely to best know how things work today (for performing the assessment), as well as what changes are likely to be successful

and where extra effort will need to be directed. “Organizational Task Breakdown,” below, provides an approach for dividing the HIPAA work load into logical components.

Organizational Task Breakdown

Department	Task
HIM, patient access, patient financial services	• Define designated record set and formal record processing procedures • Revise authorization form, policy, and procedure • Define permitted uses and disclosures for treatment, payment, and operations • Develop policy on verification of identity and authority • Address minimum necessary disclosure and request requirements • Develop policy and procedure on right to request access, amendment, and accounting for disclosures
Clinicians	• Define policy and procedure on opportunity to object to uses and disclosures (facility directory, involvement in care) • Develop policy and procedure on right to request restrictions and confidential communications
Human resources	• Assist in addressing minimum necessary use requirements • Review personnel security policies and procedures • Ensure policy and procedure on access authorization, establishment, and modification • Refine sanction policy • Ensure nonretaliation statement is supported • Work on uses and disclosures for whistle-blowers and victims of workplace crime • Develop termination checklist, policy, and procedures • Address group health plan issues
Risk management/patient relations	• Develop policy and procedure on privacy complaints • Coordinate privacy complaints with security incidents • Develop mitigation issues
Contracts/materials management	• Develop policy and procedure on disclosures to business associates • Develop and negotiate business associate contracts
Security	• Define incidental disclosures and safeguards • Address physical security (including disposal of trash and devices) • Develop policy and procedure on media controls • Address workstation use and location
Information technology	• Address certification • Develop access controls

	• Ensure audit trails are in place • Develop policy and procedure on e-mail and fax transmissions • Address contingency planning, configuration management, entity authentication, and network controls
Information privacy/security officials	• Establish policy and procedure guidelines, policy on changes, and documentation requirements • Develop notice of privacy practices • Conduct covered entity analysis • Perform risk analysis • Develop policy and procedure for requirements relative to fund raising and marketing • Address research issues, deidentification, and limited data set • Develop internal audit and ongoing compliance monitoring
Education department	• Develop education and training materials • Build awareness

Truly understanding the privacy rule and making it effective requires designing solutions for your organization. Creating policies and procedures and training materials to address HIPAA requirements will not guarantee compliance or adequately educate staff. Policies need to provide managerial guidance and procedures need to explicitly describe issues such as how the notice of privacy practices will be provided, how business associates will be identified, or that physicians need to document when harm may arise from patient access to certain information. Training needs to reflect the specific policies and procedures of the organization. And both need to be tracked and managed on an ongoing basis.

Get Outside Help

For those organizations that started preparations a year or two ago, the current challenge may be to finalize policies and procedures and get them approved. For those on the fast track, it may be necessary to buy policy and procedure templates to jump start the process. In both cases, policies and procedures need to be:

- **Reflective of the HIPAA standards while also reasonable for the organization.** A policy and procedure written for implementation on April 14, 2003, may need to be modified after it has been in practice for a while. If it is a struggle to get all parties to agree to specific wording, it may be better to be more general now and refine items later. If the organization is faced with adopting a set of templates, the templates may need to be altered after a few months of use. Keep in mind that policy and procedure templates should allow for variations so the organization can fill in its requirements. Templates should reflect operational issues, not just regulatory requirements.
- **Written clearly and simply.** HIPAA requires certain documents to be written in "plain language," and this can be applied to policies and procedures as well. Regardless of the educational level of the work force, everyone appreciates simple and straightforward instructions and explanations. Experts recommend writing such documents at the fifth-grade reading level. In fact, some have suggested finding a fifth-grade teacher to help with the drafting.
- **Approved in a timely manner.** If the organization typically requires multiple levels of approval for policies and procedures or some employees become more focused on the granular aspects of policies and procedures, it may be necessary to find ways to summarize the essence of the documents and engage the more focused individuals prior to final approval. The "Policy Summary and Approval Form," below, can serve as a template for a policy and procedure summary that may aid in streamlining approval for the volume of policies and procedures required by HIPAA.
- **Tracked and monitored to ensure training and ongoing compliance.** Those on the fast track may need to design ongoing compliance after the initial round of policy drafting has been completed. To the extent that ongoing compliance can be built into the policies and procedures, however, it is more likely such ongoing activity will be easier to accomplish.

Policy Summary and Approval Form		
Policy Name: **Executive Sponsor:**	**Type:** **Status: __ New __ Revision**	**Number:** **Date:**
Summary: *(States the essence of the policy and procedure in two to three sentences.)*		
Effect: Affected Components: *(Identifies classes of workers and/or departments most affected.)* Operations: *(Highlights most critical elements that positively and/or negatively affect the way the organization functions.)* Financial: *(Identifies operational and capital cash outlays required, as well as any return on investment and/or loss avoidance that can be quantified.)*		
Risk Assessment: *(Briefly describes the risk of not implementing the policy and procedure and the residual risk after implementation. Risk may be described as high, medium, or low; or a formal risk analysis that rates probability of occurrence and effect may result in a numeric scale.)*		
Reason: *(Describes why the policy and procedure are created/revised [such as the HIPAA standard being met]. Should identify broadest scope of requirements addressed.)*		

This sample form was developed for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local, state, and federal law.

Start with a Plan

Much like the assessment, taking the time to establish a privacy compliance plan can seem like an unnecessary and time-consuming step at this stage of the game. However, without a plan, steps may be forgotten, efforts duplicated, and rework required. A fast-track approach suggests many hands performing many tasks simultaneously. In general, this approach requires even more choreography than if tasks are performed sequentially by a few.

Typically, a HIPAA project starts with assessment and moves through stages of project planning, selecting tools, designing solutions, developing policies and procedures, acquiring necessary technology, training staff, implementing new operations and work flows, and establishing ongoing compliance monitoring. For those on the fast track, consider using a matrix approach in which tasks are completed concurrently: Training will be occurring as the assessment, solution, and policies and procedures are designed (don't forget to track this training so it "counts" for HIPAA); department managers will need to conduct the implementation; the information privacy and security officials will need to coordinate content; and the project manager will need to keep the project on track.

A project plan inherently charts progress toward a goal. Whether your organization is on the fast track or not, everyone needs the sense of accomplishment that comes from checking off completed tasks.

Margret Amatayakul *(margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.*

Web Extras!

See also Staff Discovery Tools

Article citation:
Amatayakul, Margret. "On the Fast Track to Privacy Rule Compliance." *Journal of AHIMA* 74, no.2 (2003): 16A-D.