Ready, Set, Assess! An Action Plan for Conducting a HIPAA Privacy Risk Assessment

by Gordon J. Apple, JD, and Mary D. Brandt, MBA, RHIA, CHE

Now that the privacy regulations are here to stay, it's time to conduct a HIPAA privacy risk assessment. Here's a step-by-step approach to planning and conducting an assessment for institutions of all sizes.

Given the complexity of the HIPAA privacy regulations and the significant impact they will have on the way healthcare organizations do business, now is the time for HIM professionals to determine what they and their organizations need to do to comply. Regardless of any changes that the Bush administration or others hope to make to the regulations, the reality is that covered entities (CEs) should not delay in getting ready for HIPAA. A key preliminary step toward the goal of implementation is conducting a comprehensive HIPAA privacy risk assessment.

This article describes a phased risk-assessment approach that institutions of any size can follow. Key benchmarks let you measure where your organization stands and where it needs to go, and common-sense tips for planning and conducting a risk assessment are provided.

Before You Start

It is difficult to begin the risk assessment process without understanding the HIPAA lexicon and fundamental concepts. Accordingly, before starting your HIPAA privacy risk assessment, review the regulations generally, with an intensive review of five specific regulatory sections:

- §160.103 contains key definitions on the applicability of HIPAA
- §164.501 outlines definitions specifically related to the privacy standards
- §164.502 sets forth "general rules" for uses and disclosures of protected health information
- §164.514 contains specific requirements relating to use and disclosure
- §164.530 outlines the administrative requirements that CEs will have to meet

Once you have an understanding of these essential components of the HIPAA structure, the remaining pieces of the jigsaw puzzle should begin to fit into place. (See "A Closer Look at the Regulations.")

Getting Your Privacy Risk Assessment Started

After a thorough review of the privacy regulations, you are ready to begin your risk assessment.

The process begins with preliminary organizational and educational tasks and concludes with a blueprint for the development and implementation of a HIPAA privacy compliance program. This four-step risk assessment process is inherently scalable.

Phase 1-The Right People

The privacy standards require CEs to designate a privacy official or officer. The privacy officer will be responsible for the development and implementation of the organization's HIPAA privacy compliance efforts and serve as the "brain trust" for institutional leaders and staff.

Phase 1 Benchmarks
• designate privacy official • educate and get buy-in of senior and middle management • appoint and hold initial meetings of privacy committee

Large organizations may have a full-time chief privacy officer and numerous others at the entity or department level. A small hospital or clinic may satisfy this requirement by bestowing the title on its HIM director. The privacy official should be at a high level, credible, and have a good understanding of patient data and how it is used throughout the organization.

Regardless of organizational size, the privacy official needs to be the first person to get his or her arms around the general requirements of HIPAA. This means developing a thorough understanding of HIPAA's notice and consent requirements, patient rights, and business associate issues. In particular, the privacy official should strive to gain an early "big-picture" view of what these various requirements will mean to the organization.

Once educated, the privacy official should ensure that upper and middle management are informed of basic HIPAA privacy requirements and the proposed process that will be followed in development and implementation of a compliance program. The ongoing support of top management in the compliance process is essential.

Once the privacy officer has a better understanding of the task at hand, a risk assessment team can be assembled. In larger organizations, it is expected that the privacy officer will be supported by the efforts of one or more HIPAA compliance committees that will also participate in designation or approval of the risk assessment team.

The risk assessment team should include people familiar with the basic flow of protected health information (PHI) in a variety of areas, including but not limited to:

- HIM
- clinical care (MDs, RNs, lab, and other ancillary areas where data is used/disclosed)
- administrative transactions (patient registration and appointments, fund raising, etc.)
- financial transactions (payment, health plan authorizations, medical necessity reviews)
- research (institutional review board, research coordinators)
- education (residents, etc.)
- public health (cancer registry, communicable disease reporting requirements)
- general corporate (information technology, human resources, legal)

Phase 2-Conducting An Initial Risk Assessment

It is important to remember that the government recognizes that one size does not fit all. The preamble to the final rule states:

Wherever possible, the final rule provides a covered entity with flexibility to create policies and procedures that are best suited to the entity's current practices in order to comply with the standards, implementation specifications, and requirements of the rule. This allows the covered entity to assess its own needs in devising, implementing, and maintaining appropriate privacy policies, procedures, and documentation to address these regulatory requirements.

Phase 2 Benchmarks
• identify primary areas for review within the framework of enumerated HIPAA requirements • develop a Phase 2 work plan

- map the internal and external flow of PHI
- identify the technical infrastructure
- inventory existing policies and procedures
- prepare Phase 2 summary reports

In practical terms, this means that in individualizing the risk assessment process for an organization, it is important to understand just how big an organization is. If your organization operates in numerous states and has an operating budget in the billions, then your risk assessment process should be extensive and sophisticated. You're likely to rely on sophisticated information technology techniques in gathering and analyzing risk assessment data. On the other end of the spectrum, if you work at a small rural clinic, you will likely rely on doing what is quick, efficient, and practical.

This part of the risk assessment should be designed to identify primary areas for review within the framework of the enumerated HIPAA requirements. At this point, your goal is to come away with a big-picture view of what is going on in the organization and how existing processes, policies, and procedures roughly match up with HIPAA privacy requirements.

"Phase 2-Mapping Information Flow," and "Key Phase 2 Tasks for Implementation," contain a listing of general Phase 2 tasks that are tied to or support the implementation of key HIPAA requirements. The first task (and probably one of the most challenging) is mapping the internal and external flows of PHI.

The time and difficulty of this task will likely be a function of an organization's size and complexity. The remaining tasks involve identification of the technical infrastructure and the inventory of existing polices and procedures.

The goal for all Phase 2 tasks is the development of summary documents that tell an organization what appears to be going on and the development of checklists that can be used in Phase 3 for department-level reviews and the eventual gap analysis.

The privacy officer and the privacy committee (if there is one) should oversee this initial data/information-gathering process. Then, develop a work plan that addresses who is responsible for conducting each element of the Phase 2 analysis, the expected work product, and the timeline for completion. Consider doing a test run to determine the most effective way to gather the Phase 2 data. An initial beta test will allow you to modify the process to fit institutional needs and quirks. Obviously, some tasks will be difficult, depending on the size of an organization.

The Phase 2 summary reports should be shared with both upper-level and line management to discover if anything significant has been missed. After filling in the initial assessment gaps, the organization can then proceed with the development of department-level risk assessment checklists/forms (tools). Adopt a consistent and uniform analytical approach for each area in a facility or department that merits review.

Phase 3-The Next Level

In Phase 3, the risk assessment should move from the macro-organizational level to the micro-departmental level. With the data gained through the Phase 2 analysis, CEs will be able to develop uniform assessment tools that department administrators can use to gather detailed data. The Phase 3 timeline should be relatively short if you have developed easily understood assessment tools. For a sample department-level assessment tool designed to track the flow of PHI, go to AHIMA's Web site at www.ahima.org. Click "Ready Resources," then "Journal of AHIMA." Select "Feature Articles" and then select this article. Look for a link to this tool in the online version of this article.

The goal of the Phase 3 analysis should be a report that clearly identifies existing PHI data practices across the spectrum of organizational activities. This "gap analysis" report should contain an inventory of existing policies and procedures and a chart that compares existing practices to those required under HIPAA. The report should contain an inventory of IT/IS equipment and practices used in the capture, storage, and transmission of PHI. Finally, the report needs to provide an easily understood set of maps that present PHI flow.

Phase 3 Benchmarks

- develop Phase 3 risk assessment tools
- develop Phase 3 work plan
- develop Phase 3 report

Phase 4-A Plan for the Future

A final step in the risk assessment process should be establishing priorities to guide the development and implementation of a HIPAA privacy compliance plan.

Phase 2 Benchmarks

- develop priority (risk ranking) checklist
- create work plan for Phase IV analysis
- prepare Phase IV report

Based on the Phase 3 report, determine the areas that present the greatest potential compliance risks. Think of the documentation of this final risk assessment effort as an addendum to the more comprehensive Phase 3 report. In effect, the Phase 4 report should be an executive summary of conclusions, options for action to achieve HIPAA compliance, and recommendations on resource allocation.

Establishing Priorities

It may be necessary to apply a weighting factor to areas of concern to identify and manage development and implementation priorities. Prime candidates are those areas in a facility that either have frequent access to PHI or areas where access is not frequent, but where failure to comply with the privacy regulations could lead to severe or significant problems. Develop some common-sense checklists.

For example, consider the issue of business associates, which come in all stripes and colors. A remote coder who is an independent contractor would be a business associate. The failure of that individual to comply with HIPAA privacy regulations could lead to problems. Given the amount of PHI being provided to the coder, he or she would be given a high frequency score.

Now think of your professional liability legal counsel. Although defense counsel may not have a lot of PHI on computer hard drives, any PHI that is there may be highly sensitive. Accordingly, defense counsel would be given a high severity score.

The HIPAA risk assessment process serves at least three very useful purposes for healthcare organizations and other covered entities. Primarily, the mere act of going through a risk assessment will sensitize organizational leaders to the requirements and scope of the HIPAA privacy standards. More importantly, however, the risk assessment process serves as a useful institutional checkup for privacy practices in the digital age. Finally, the process provides the necessary blueprint for action in the development and implementation of a HIPAA privacy compliance program.

HIPAA's Basic Framework

Before beginning the risk assessment process, it is important to understand HIPAA's framework. The law's preamble lists its three essential purposes:

- to protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information

- to improve the quality of healthcare in the US by restoring trust among consumers, healthcare professionals, and the multitude of organizations and individuals committed to the delivery of care
- to improve the efficiency and effectiveness of healthcare delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, and organizations and individuals

HIPAA seeks to meet these goals through the enumeration of regulatory standards, implementation specifications, and requirements. The regulatory standards and implementation specifications will preempt less stringent state laws in most circumstances. 45 Code of Federal Regulations (CFR), Part 160, outlines the general administrative requirements. Part 160 defines who is covered by HIPAA and certain key terms.

The privacy regulations, labeled "Privacy of Individually Identifiable Health Information," are found in 45 CFR Part 164, Subpart E. Sections 164.500 to 164.534 outline the specific requirements that CEs will need to follow. Except for §§501 and 534, each of the 17 sections contains regulatory standards, and many standards also have implementation specifications. For example, under §164.506, the standard requires "consent for uses or disclosures to carry out treatment, payment, or health care operations." One of the implementation specifications under that standard outlines specific "content requirements."

For the full text of the privacy regulations, go to the Department of Health and Human Services' comprehensive HIPAA Web site at http://aspe.os.dhhs.gov/admnsimp/.

A Closer Look at the Regulations

Before you launch your risk assessment, review the regulation, paying special attention to these sections:

§160.103-Definitions

In alphabetical order, some of the most significant terms under §160.103 to fully understand before beginning a risk assessment are:

- business associate
- covered entity
- healthcare
- health plan
- healthcare provider
- health information
- implementation specification
- standard
- transaction
- work force

Think of these terms in the real-world context in which you operate. Covered entities are essentially all of the players in direct healthcare delivery and payment that transmit health information in electronic form to carry out financial or administrative activities related to healthcare. In a few cases, it is possible to be a healthcare provider and not be a covered entity. For example, some small healthcare providers may not use electronic transactions and thus would not be covered by HIPAA.

§164.501-Definitions

The definitions contained in §164.501 are specific to the privacy regulations. Prior to conducting a risk assessment, review the definitions that apply to your facility. Likely suspects include:

- individually identifiable health information
- covered functions
- designated record set
- direct treatment relationship
- indirect treatment relationship
- disclosure
- healthcare operations
- marketing
- organized healthcare arrangement
- payment
- protected health information
- psychotherapy notes
- required by law
- research
- treatment
- use

Once HIM professionals gain a contextual understanding of HIPAA's definitions, they will be in a much better position to engage in the risk assessment process. Based on the preceding definitions, sections §§502, 514, and 530 contain the general requirements that will help identify the areas for review in the institutional risk assessment process.

§164.502-Uses and disclosures of protected health information: General rules

This section provides the general rules that CEs must follow when using or disclosing PHI. The first part of this section outlines "permitted uses and disclosures" and then addresses "required disclosures." 502(b) presents the "minimum necessary" standard, but then notes that it does not apply to "disclosures to or requests by a health care provider for treatment." (§164.502(b)(2)(i).)

In the risk assessment context, the most significant aspect of §502 relates to business associates. Section 502 (e) allows a CE to disclose PHI to a business associate and to allow a business associate to either "create" or "receive" PHI on its behalf. To do this, however, the CE must have obtained "satisfactory assurance that the business associate will appropriately safeguard the information." The satisfactory assurances must be contained in a contract or other written agreement or arrangement. Identification of business associates will be a key challenge in conducting a risk assessment.

§164.514-Other requirements relating to uses and disclosures of PHI

In many ways, section 514 contains many of the most important requirements under the privacy standards. From setting out the standard for deidentification of PHI to the standard for verification of the identity and authority of a person accessing PHI, this section is a "must read" for HIM professionals. In addition to verification and deidentification standards, §514 contains standards and implementation specifications for minimum necessary requirements, uses and disclosures of PHI for marketing, uses and disclosures for fund raising, and use and disclosures for underwriting and related purposes.

§164.530-Administrative requirements

§530 outlines many of the key components that all CEs will have to follow, regardless of size. In addition to the requirement that a "privacy official" be designated, §530 outlines numerous other standards, including those relating to safeguards and policies and procedures. Significantly, the safeguards standard references the yet-to-be-published final HIPAA security standard in stating that a

CE "must have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information."

Phase 2-Mapping Information Flow

Phase 2 Tasks	General Process	Goal
M. Identify how PHI is used/disclosed for "treatment, payment and health care operations."	Map internal data flow according to payment, treatment, and healthcare operations.	Summary report to share with senior management. Tasks M-1 to M-3 can be seen as subsets of the general mapping task. The report should contain both written and visual depictions of data flow.
M-1. Identify relationships with other covered entities.	Map flow of data to and from other CEs, such as health plans and clearinghouses	Summary report that identifies the major players an organization does business with.
M-2. Identify relationships with business associates.	Map flow of PHI to and from business associates.	Summary report that identifies business associates by category. In the hospital setting, typical business associates include information systems vendors, medical transcription companies, release of information companies, off-site record storage vendors, contract coders, consultants, and collection agencies.
M-3. Identify how PHI is captured.	Map points where PHI enters the institution.	Summary report that identifies how PHI is first collected. This report will overlap with some of the preceding tasks.

Technical infrastructure	Identify IT hardware and IT communication components used in the capture, storage, and transmission of PHI.	A summary report that identifies the equipment/technology used by institutions involved in the flow of PHI (for example, workstations, PCs, servers, PDAs, LANs, WANs, intranets, and Internet). Existing safeguards, such as access and authentication controls, should also be identified.

Key Phase 2 Tasks for Implementation

Phase 2 Tasks	General Process	Goal
Patient access rights	Identify existing policies, procedures, and access protocols.	Summary report that notes the respective HIPAA requirements and identifies existing policies and procedures that either meet the requirement or will have to be amended to meet them.
Minimum necessary requirement	Identify existing mechanisms to ensure that staff members, physicians, and outside requesters have access only to the information needed to do their jobs or fulfill the purpose of their request.	.
Patient consent requirement	Identify existing consent documents (such as the general consent form signed during the registration process), policies, and procedures.	
Notice of information practices	Identify existing notice documents and related policies and procedures.	

Right to an accounting of disclosures	Identify existing process for tracking non-routine disclosures of PHI.	
Right to agree or object to certain disclosures	Determine if existing policies and procedures apply.	
Right to specific authorization for non-routine disclosures	Determine if existing policies and procedures apply; collect existing authorization forms.	
Patient right to request restrictions on disclosure	Determine if existing policies and procedures apply.	
Patient right to request amendment/correction	Identify existing policies and procedures.	

Steps for Follow-up

In developing a risk assessment plan, think in terms of deliverables. For example, consultants responding to an RFP for a HIPAA risk assessment may list the following deliverables:

1. Itemize the specific forms and notices that the privacy standards require CEs to have. This list would include:

- individual consent form for use/disclosure of PHI in treatment, payment, and healthcare operations
- notice of information practices
- individual authorization form for CE’s use or disclosure of PHI for which authorization is required
- individual consent form for release of psychotherapy notes
- individual "opt-out" form regarding fund raising by the CE
- business associate contracts/agreements
- work force training certification form

2. Identification of business associates

- priority list of business associates by type and size
- standard business associate contracts or contract clauses
- standard RFPs with HIPAA due diligence questions for new business associates

3. Inventory (key to HIPAA requirements) of existing policies and procedures-corporate, institutional, and departmental

4. Development of HIPAA-specific policies and procedures

- uses and disclosures by CE requiring an opportunity for the individual to agree or object
- individual request for an accounting of disclosures of PHI
- individual request for privacy protection for PHI used in treatment, payment, and healthcare operations
- individual request to amend PHI

Online Only

A sample department-level risk assessment tool to use with this article is available in MSWord format here. To view the sample, simply click the link.

***Gordon Apple** is an attorney in St. Paul, MN. In addition to his health law practice, he is a frequent speaker on HIPAA and other health law topics at professional and corporate meetings. He can be reached at Gapple@HealthLawGeek.Com. Mary Brandt directs the regulatory compliance practice at Outlook Associates, Inc., a California-based healthcare and information technology consulting firm. The former director of policy and research for AHIMA, she is a frequent speaker on HIPAA and other regulatory and HIM practice issues at professional meetings. She can be reached at mbrandt@outlookassoc.com.*

Article citation:
Apple, Gordon J. and Mary D. Brandt. "Ready, Set, Assess!: an Action Plan for Conducting a HIPAA Privacy Risk Assessment." *Journal of AHIMA* 72, no.6 (2001): 26-32.