New Privacy Officer's Game Plan

by Jill Callahan Dennis, JD, RHIA

The HIPAA-mandated privacy officer role offers a new opportunity for HIM professionals. What skills are required, and what needs to be done first? This article answers these questions.

As healthcare organizations roll out their plans for HIPAA implementation, many HIM professionals will find themselves stepping into the role of privacy officer for their entire organization. What does this role require, and what skills do HIM professionals bring to the task? In this article, we'll review what the proposed regulations require and start to create the privacy officer's game plan.

Privacy versus Security?
HIPAA's final privacy rule requires healthcare provider organizations (and other covered entities) to designate someone to serve as a privacy official.1 Beyond that, however, organizations have received little explicit guidance as to structuring this newly required role.

Many healthcare organizations are beginning to evaluate their options for meeting this requirement, and the options are numerous. What makes the situation somewhat more confusing is that the proposed information security regulations also require that someone (or some organization, such as a committee) be in charge of information security. That person's or group's role is to "manage and supervise the execution and use of security measures to protect data, and to manage and supervise the conduct of personnel in relation to the protection of data."2

Can (or should) one person be in charge of both issues-privacy and security? Is the "privacy official" function best accomplished by an existing staff member, or do we need to find a new skill set from outside of the existing staff? Moreover, is this a full-time job in itself, or can the functions of a privacy officer be blended with other duties? Are certain staff members' backgrounds more conducive to success in the role than others? And if we are considering this role ourselves, what will be expected of us?

First, we need to look at the "givens"-what exactly is required by the privacy rule. This provides us with a good grounding in the minimum duties of the privacy officer.

What Is Required?
Section 164.530(a) of the final privacy rule outlines the basic requirement for a privacy official: "A covered entity must designate a privacy official who is responsible for the development and implementation of the privacy policies and procedures of the entity."

Covered entities must also designate a contact person or office to be responsible for receiving privacy-related complaints and for providing information about information-handling matters-such as the required notice of information practices. Although this contact person or office is not required to the privacy official, it (or he or she) may be.3

The final rule outlines numerous policies and procedures that covered entities must have in place. Because the development and implementation of these policies and procedures are mandated responsibilities of the privacy official, at least four important duties are implied for the new privacy officer. (See "A Privacy Officer's Duties," page 35.) The "implied" duties offer a potentially useful game plan for defining and structuring a role for the new privacy officer.

Should You Be the Privacy Officer?
The regulations tell us a little about the potential scope and duties of a privacy officer, but they don't specifically dictate the skill

set required-or whether we can find this skill set within existing staff. Nonhealthcare corporations hiring privacy officers have struggled with this question as well.

Obviously, a healthcare organization's needs for a privacy officer will be slightly different than those of other businesses, in part because of HIPAA's framework. Nevertheless, an understanding of applicable laws, a sensitivity to public relations, and at least a basic understanding of information technology seem fundamental. (See "A Privacy Officer Skills Wish List," page 37, for skills a privacy officer may require.)

the privacy officer in the corporate world

Is being the privacy officer a full-time job? Healthcare models are still rather rare, but in the corporate world, the answer for many high-tech companies appear to be "yes."

Outside of healthcare, an increasing number of companies have turned to a new corporate player, often called the chief privacy officer (CPO), to prevent legal or public relations and marketing disasters. These CPOs are charged with making sure companies' privacy policies are adequate and are followed. They also are responsible for knowing privacy-related laws and regulations and reviewing proposed business plans to sniff out potential conflicts with internal privacy policies and applicable laws and regulations.

Although some CPO appointments stem from settlements of privacy infringement lawsuits, many companies are beginning to see value in having someone on board with the vision to anticipate potential privacy problems and to call a halt when a proposed use of data may hurt the company as well as the customer.

It's not just a matter of protecting yourself from lawsuits, one expert says. "The battle for competitive advantage is going to increasingly be fought with a closer relationship to customers, and the only way that's going to work is if customers trust companies with their data," Ward Hanson, a lecturer at Stanford's Graduate School of Business, told Knight-Ridder reporters recently. "So smart companies will have these skills in-house and will invest the resources necessary to make it an important function."11

In most published models, the CPO reports to the CIO or CEO. The job requires a certain amount of fortitude and high-level authority. "There's so much hidden value in personal information, and you're asking people to restrain themselves in the use of it," said Stephanie Perrin, CPO of Zero-Knowledge Systems Inc., a Montreal-based global privacy company, in an article in eWeek. "You have to push back and say, 'I don't care how interesting it would be to gather this data. We said we weren't going to do it."12

There are, however, some potential down sides to designating anyone solely as a privacy officer and having that be their only job function, Julia Johnson, privacy coordinator for Bank One Corp., told the ABA Banking Journal. One risk is that other parts of an organization might feel that they had been "let off the hook." That's why she decided not to have a privacy staff. "My job is to be the one who maintains an enterprise-wide perspective of the data flows within our company," Johnson explains. "For me, this is kind of like being an orchestra conductor. I don't play any of the instruments, but I have to make beautiful music. I am a champion, part of the team, a coach, a subject matter expert, and a consumer advocate."13

HIM professionals, by virtue of their training and their experience, have many (if not most) of the needed skills. Probably no other professionals within the organization have as full an understanding of how protected health information is used within the organization and disclosed externally.

Additionally, HIM professionals are likely the authors of many of the policies and procedures that will be affected by HIPAA. And in many organizations, they are already responsible for training staff about privacy and confidentiality-related issues.

There may well be some competitors for the role of privacy officer. Several positions within a typical healthcare organization have some (if not all) of the skills listed above:

o in-house counsel
o risk managers
o directors of compliance

o directors of medical affairs
o information systems managers
o administrators over these functional areas

The Game Plan
With the requirements in mind, we can identify at least five basic elements of the new privacy officer's game plan:

- compiling and evaluating existing policies and procedures against regulatory/legal mandates
- changing them where necessary and training staff on the changes
- understanding how information flows within (and outside of) the organization
- determining what other tasks logically fit with those mandated duties
- finding resources to assist in fulfilling the requirements

Look at Policies and Procedures
Once we have gathered a complete set of current policies and procedures for use and disclosure of information, our next step in the game plan is to determine their compliance with the final privacy rules (as well as any other applicable requirements, such as more restrictive state laws and regulations, other federal rules such as those governing substance abuse treatment program records, and so on). Key questions to aid in that evaluation would be:

- Do we have a policy or procedure to cover all required areas?
- Does that policy or procedure include all elements required by HIPAA regulations or other applicable state or federal requirements?
- Have all applicable staff, contractors, or volunteers been trained in using that policy or procedure?
- Does documentation exist that the required training has taken place?

a privacy officer's duties

Required Responsibility	Implied Duties
Development of privacy policies and procedures	1. Audit current policies and procedures to evaluate their adequacy (or whether they even exist), in light of the regulatory requirements 2. Updating/changing policies and procedures as necessary
Implementation of privacy policies and procedures	3. Train staff (or at least oversight of training) in relevant policies and procedures 4. Evaluate adherence to policies and procedures to ensure effective implementation

Revise Policies and Plan Training
The results of these inquiries will very likely indicate the need for updating or changing existing policies, developing new ones, and revising current training efforts (in content or in "reach").
Training (and periodic retraining) is an important feature of the final privacy rule. (It is also an important and required feature in the proposed information security regulations, and there may be substantial benefits in combining efforts with the information security officer in planning training that meets both requirements.) But it is insufficient to simply offer generic, "one-size-fits-all" privacy training to new employees once and then assume that the lessons have been learned.

The final rule requires job-specific training for anyone in the work force who, by virtue of his or her position, is likely to obtain access to protected health information. In other words, training must cover policies and procedures that are relevant to carrying out that work force member's function within the entity.4

The rule also addresses the timing of training. For existing members of the work force, training must occur by the date the regulations become applicable to the entity (generally 24 months after the final rules are published). For new members of the work force who join after the compliance date, training must occur within "a reasonable period after the person joins the work force."5

All such training must be documented via written or electronic record, retained for at least six years.6
As for retraining, the final regulations require that it be provided to all members of the work force who have access to protected health information, as relevant to their function within the entity, whenever privacy policies and procedures materially change.7

Understand How Information Flows
Beyond the issues of designing initial training that is relevant to the particular functions of each work force member with access to protected health information, it will be necessary to understand which member(s) are involved in each process described in all privacy-related policies and procedures.

To accomplish this, it will be necessary to identify, by job description or role, whether or not that job or role involves likely access to protected health information. If it does, what is the nature of that job's involvement in using, handling, or disclosing the information?

Compiling this information will be tedious at best, and larger organizations will find the task daunting but necessary. There are several options for gathering this information. A review of job descriptions may give some basic indications of each job's access to health information, but may not offer a complete description of the nature or extent of that access. In addition, some members of the work force may not have existing job descriptions, as defined by the final regulations. (Remember that the final regulations define "work force" as employees, volunteers, trainees, and other persons under the direct control of a covered entity, including persons providing labor on an unpaid basis.8)

Interviews with department managers and front-line supervisors may assist in supplementing the basic information found in job descriptions and may be vital in situations where job descriptions do not exist, such as for volunteers. In some cases, it may be necessary to conduct work force interviews or observe work being performed to fully understand the level and breadth of access to information.

This "information access inventory" will need to be up to date at all times, so that whenever material changes are made to policies or procedures, it will be possible to determine which members of the work force will require retraining.

who uses health information?

Here are just a few examples of acute care hospital departments or areas likely to be involved in using, accessing, processing, or disclosing protected health information:

- Health information management
- Transcription/word processing units
- Cancer and disease/trauma registries
- Information technology/services
- Nursing
- Emergency department
- Ambulatory care clinics and surgicenters
- Entity-owned physician practices
- Quality/performance improvement
- Risk management
- Case/utilization management
- Medical staff
- Laboratory
- Radiology
- Respiratory therapy
- Physical and other therapies
- All other clinical units and departments
- Special procedure areas
- Admitting/patient registration
- Patient accounting/finance
- Home care program
- Hospice program
- Volunteer department

Consider Other Likely Functions
Beyond these required and implied duties, a number of other important functions may fit within the responsibilities of the privacy officer, depending on his or her particular skill set. Reviewing and negotiating business partner contracts to bring them into compliance with the final privacy rules will be a considerable and important task, as it is likely that few existing contracts contain all necessary contractual provisions. A summary of those required provisions can be found in section 164.504(e)(2). Even if the designated privacy officer is unable to adequately review contract language or negotiate changes, he or she could

serve as the central repository for all existing contracts, facilitating the process of reviewing those agreements for any changes that may be necessary now or in the future.

The privacy officer is also likely to be responsible for cooperating and coordinating with the Department of Health and Human Services (or other agencies enforcing the HIPAA regulations) in any investigations launched in response to patient complaints. As the most knowledgeable internal contact, the privacy officer will likely be heavily involved in any investigations.

And, although the privacy officer is not required to personally conduct the training referred to above, he or she certainly has some responsibility to ensure that training-related procedures are followed. As a result, many organizations may see advantages to involving the privacy officer in performing the training. In any event, it will be important that whoever leads the training is familiar with applicable HIPAA requirements.

Does it make sense for the privacy officer to also serve as security officer, as defined by proposed information security regulations? There does appear to be some potential overlap between the roles, but there are also some important differences.

The security officer (or group charged with this responsibility) would, like the privacy officer, have some responsibility for the conduct of personnel in relation to the protection of data. However, the security officer would be required to manage the use of security measures to protect data-a role that appears to require solid technical expertise in information security.

Whether or not one person can reasonably be expected to have both the detailed technical knowledge and the "big-picture" thinking required for the privacy officer will likely be a decision that must be made by individual healthcare facilities, taking into account the available staff resources and their unique talents.

Whether or not these roles are combined, it may be wise to consider administratively grouping, as much as feasible, key information-handling departments and functions under (or alongside) the privacy officer. Such an arrangement may facilitate the process of keeping HIPAA-related policies and procedures up to date and may make ongoing training somewhat easier. Unfortunately, a large percentage of the organization's departments will fall into this category, so it will probably be impossible to group all affected departments together. See "Who Uses Health Information?" above, for a few examples of the departments that handle or use health information.

Don't forget about departments that can be expected to have access to health information, even though their jobs don't require them to use that information-such as housekeeping/environmental services staff who empty trash cans that may contain protected health information. Indeed, it may be simpler to list departments without likely access to protected health information.

Finding Useful Resources
Regardless of background, the privacy officer is likely to need the assistance of other subject matter experts within the organization. It may be useful to form an ad hoc privacy council that can offer advice and support-and many healthcare organizations will be looking for external support as well.

Oregon-based Providence Health Systems brought in consultants to look at its existing security measures and its security and confidentiality policies and then compare them with HIPAA's proposed rules. With more than 1 million enrollees and 5,500 physicians, Providence found that it needed policies to address issues such as integration of the different aspects of security and confidentiality. The group then compared its policies and procedures with what was known about HIPAA and has begun working toward compliance.9

Fortunately, numerous resources are available to assist the new privacy officer, and many of them are free or inexpensive. Numerous Web sites offer HIPAA-related information, checklists, and other resources. Healthcare publishers and associations, including AHIMA, have also delivered a wealth of articles, checklists, and practice briefs to assist in privacy-related compliance efforts.

a privacy officer skills wish list

Here are a few of the skills that are likely to be useful for anyone taking on the role of privacy officer:

- Expertise in the final HIPAA rules

- Knowledge of other applicable state and federal laws and regulations
- Understanding of how protected health information is used within your organization
- Understanding of how protected health information is disclosed outside of your organization
- Ability to communicate effectively (in writing and verbally) with all levels of the organization
- Experience and skill in dealing with patients and the public
- Experience and skill in dealing with outside regulators, surveyors, and inspectors
- Understanding of information technology
- Expertise in reviewing (and potentially drafting) contract language
- Ability to promote what may be "unpopular" positions and policy

How Will We Measure Success?

Appointing a privacy officer and simply hoping for the best won't get us where we need to go. If we are to achieve real benefits in improving privacy and confidentiality in our organizations, we need to set performance measures and benchmarks-benefits that accrue as much to the healthcare organization as to its patients. What potential performance measures might we use and track, over time, to evaluate our success? Some might include:

- tracking the numbers of breach of confidentiality/privacy infringement-related complaints
- tracking the number of claims/suits alleging confidentiality/privacy breaches
- regulatory fines related to privacy and confidentiality issues
- numbers of internal incidents involving violations of privacy policies
- percentage of work force members receiving privacy training on time (according to mandated schedules)
- percentage of work force with current privacy/confidentiality certifications on file10
- accrediting agency citations involving privacy/ confidentiality

HIPAA presents HIM professionals with many new challenges and as many opportunities. The privacy officer will play a key role in contributing to the organization's success or failure. By defining the appropriate scope of duties for that officer, fashioning a realistic game plan to guide his or her activities, finding the right person for the task, and then equipping them with appropriate resources, we increase our chances of a successful transition to a HIPAA-compliant organization.

Notes

1. See section 164.530(a)(1) of the final privacy rule and section 164.520(c)(2).
2. See section 142.308(b)(1) of the proposed information security standards.
3. See section 164.530(a)(2).
4. Training requirements are addressed in section 164.530(b).
5. See section 164.530(b)(2).
6. See section 164.530(b)(2)(ii) and (j).
7. See section 164.530(b)(2)(i)(C).
8. "Work force" is defined in section 164.103.
9. Lentz, Rebecca. "Privacy matters." Modern Physician 4, no. 5 (2000): 39.
10. Fuller, Sandra. "Setting the Foundation for Compliance through Effective Policies." Presentation at 2000 HIPAA Conference of the Joint Healthcare Information Technology Alliance, Chicago, September 28, 2000.
11. Steen, Margaret, and Elise Ackerman. "Companies Hiring Chief Privacy Officer." Knight-Ridder/Tribune News Service, July 12, 2000.
12. Kosan, Lisa. "E-biz execs guard Net privacy-Cops oversee companies' personal data policies." eWeek, August 14, 2000, p. 60.
13. Cocheo, Steve. "Making privacy a brand issue at Bank One." ABA Banking Journal 92, no. 7 (2000): 20.

Jill Callahan Dennis *is principal of Health Risk Advantage, a Denver-based risk management consulting firm, and a member of the Journal of AHIMA's advisory board. She is the author of Privacy and Confidentiality of Health*

Information, published September 2000 by Jossey-Bass Publishing and the AHA Press.

Article citation:
Dennis, Jill Callahan. "The New Privacy Officer's Game Plan." *Journal of AHIMA* 72, no.2 (2001): 33-37.