SESSION 5
The New Privacy Officer’s Game Plan

Jill Callahan Dennis, JD, RHIA
Principal
Health Risk Advantage
Parker, CO
HIPAA’s (the Health Insurance Portability and Accountability Act’s) proposed Privacy Rule requires healthcare provider organizations (and other covered entities as defined by the rule) to designate someone to serve as a privacy official. Beyond that, HHS offers little explicit guidance to organizations in how best to structure this newly required role.

Many healthcare organizations are beginning to evaluate their options for meeting this requirement, and the options are numerous. Is this 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?

What expectations should we have of this person, and if we are considering this role ourselves, what will be expected of us? To answer these questions, we must start with the regulations themselves, and then construct a role description for the privacy officer that not only meets those requirements, but also makes sense within our own organizational culture. In other words, we need a realistic game plan for that privacy officer.

Too often, regulatory compliance is largely a “paper exercise” in our organizations. Some do only what is required to pass muster during accreditation and regulatory surveys and inspections. Often that means that we put many things on paper that have no real relationship to what we do in practice. And although that may permit us to skate precariously through a survey, it can put us at risk when something goes wrong, and it is discovered that we say one thing on paper, but do quite another.

The risks associated with mere “paper compliance” include at least the following:

- **Regulatory Risks**—such as civil monetary penalties levied for noncompliance by regulatory bodies such as the Department of Health and Human Services, and fines or even imprisonment for “knowingly” using or disclosing identifiable health information in violation of HIPAA²;
- **Risks of Lawsuits**—when an organization’s actual practices fail to comply with its own stated policies and procedures, that can often be used as powerful evidence of a breach of the standard of care. Juries can be very unsympathetic to organizations that give only lip service to their own policies and procedures;
- **Public Relations Risks**—Patient and public dissatisfaction, and damage to the organization’s reputation, are likely results when examples of information mishandling become publicly known;
- **Risks to Staff Morale**—Staff members are unlikely to view patient privacy and confidentiality as serious and important subjects, if related policies and procedures are not enforced consistently. Inconsistent or only selective enforcement can result in perceptions of unfairness, and can open the organization up to challenge when disciplinary actions are attempted.

Care and forethought in planning the role of the privacy officer can help minimize these risks, by structuring the role in a way that communicates its importance and authority. Although no one organizational model will fit all settings, we’ll examine several options for structuring the role in ways likely to promote positive results.

But first, it is useful to review 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 164.518(a) of the proposed 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 may be.

The proposed rule outlines numerous policies and procedures which 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 official:
These “implied” duties offer a potentially useful game plan for defining and structuring a role for the new privacy officer.

As for the types of policies and procedures required by the regulations (and therefore an area of focus for the privacy officer), they include the following:

1. Procedures identifying who, within the covered entity, determines what information should be used or disclosed consistent with the “minimum necessary” standard of the regulations;
2. Procedures to ensure that the persons identified above actually do make those “minimum necessary” determinations when required;
3. Procedures for making those “minimum necessary” determinations individually, within the limits of the entity’s technological capabilities;
4. Procedures to permit individuals to request restrictions on the uses and disclosures of their protected health information;
5. Procedures to ensure that, if any restrictions are agreed to by the entity, the restrictions are reduced to writing or otherwise documented;
6. Procedures for honoring the above-mentioned restrictions on uses and disclosures;
7. Procedures to notify others to whom such information is disclosed of any such restrictions;
8. Policies and procedures governing the process of obtaining authorization for use/disclosure of information, when such authorization is required—such as:
   - requests from individuals,
   - requests from covered entities not related to treatment, payment, or health care operations,
   - disclosures to health plans prior to the individual’s enrollment,
   - disclosures to employers for use in employment determinations,
   - uses/disclosures for fundraising purposes,
   - uses/disclosures of psychotherapy notes, and
   - uses/disclosures of research information unrelated to treatment;
9. Policies and procedures for determining the adequacy and completeness of authorizations received by the entity;
10. General policies and procedures for handling the following types of information requests, when written authorization is not required:
   - disclosures for treatment, payment, and health care operations,
   - disclosures to business partners, including monitoring and mitigation,
   - disclosures to public health authorities,
   - disclosures and uses for health oversight activities,
   - disclosures and uses for judicial and administrative proceedings,
   - disclosures to coroners and medical examiners,
   - disclosures for law enforcement purposes,
8. disclosures and uses for governmental health data systems,
9. disclosures of directory information,
10. disclosures and uses for research purposes,
11. disclosures and uses in emergency circumstances,
12. disclosures to next-of-kin, and
13. uses and disclosures for specialized classes such as military purposes, Department of Veterans Affairs, intelligence community, and the State Department13;
11. Procedures for providing a notice of information practices to individuals, including the identity of persons responsible14;
12. Policies and procedures for granting and denying individuals access to their protected health information, including the identity of persons responsible, grounds for denying requests, and copying fees (if any)15;
13. Procedures to give individuals an accurate accounting of disclosures of their protected health information (only for disclosures for which an accounting is required), and the persons responsible for accomplishing this16;
14. Procedures for handling requests for information amendments and corrections, including procedures for accepting, denying, and acting upon such requests, and the persons responsible for these matters17;
15. Procedures for training the workforce on privacy-related policies and procedures18;
16. Procedures for verifying the identity and/or authority of persons requesting protected health information, where such identity or authority is not known to the entity19;
17. Procedures for an individual to file a complaint alleging that the covered entity failed to comply with the regulations20;
18. Policies and procedures for applying sanctions against members of the workforce who violate required practices21;
19. Procedures for mitigating, to the extent practicable, any deleterious effect of any use or disclosure of protected health information in violation of these rules22;
20. Procedures describing how access to protected health information is regulated by the covered entity and its business partners, including safeguards used23; and
21. Record retention policies for requests for restrictions, business partner contracts, authorization forms, sample notices of information practices, accountings of uses and disclosures (where required), written statements related to individuals’ requests for information, documents relating to denials of requests for amendment and correction, workforce training certifications, and privacy-related complaints received by the covered entity24.

These are the policies that are either required or implied by the draft Privacy Rule. It is important to remember that this list could change with the final rules, once they are published. Nevertheless, compiling all existing policies and procedures on these subjects offers a good starting place for the new privacy officer seeking a “jump start” on his or her duties.

THE GAME PLAN

Compile and evaluate all relevant existing policies and procedures

There may well be additional existing facility policies and procedures that should be examined by the new privacy officer in addition to those listed above. 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). This is often called a “gap analysis.” Key questions to aid in that evaluation follow:

1. Do we have a policy and/or procedure to cover all required areas?
2. Does that policy and/or procedure include all elements required by HIPAA regulations, or other applicable State or Federal requirements?
3. Have all applicable staff, contractors, and/or volunteers been trained in using that policy and/or procedure?
4. Does documentation exist that the required training has taken place?
Begin developing new or revised policies and procedures, where needed, 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 proposed privacy rules. (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 to assume that the lessons have been learned. The proposed rules require job-specific training for anyone in the workforce who, by virtue of their position, is likely to obtain access to protected health information. In other words, the training must cover the policies and procedures that are relevant to carrying out that workforce member’s function within the entity.23 For example, nurses are likely to need training that covers the importance of being aware of one’s surroundings when discussing patient information on the unit, while housekeeping personnel shouldn’t need that information in their confidentiality training (as their job does not involve the need to discuss patients). However, housekeeping staff would need to learn of proper ways of disposing of confidential information that has been discarded.

The proposed regulations also speak to the timing of that training. For existing members of the workforce, that 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 workforce, joining after the effective date of the regulations, that training must occur within “a reasonable period after the person joins the workforce.”24 All such training must be documented via a signed certification, stating the date of the training, and that the person completing the training will honor all of the entity’s applicable policies and procedures. That certification must be re-signed at least every three years.25 As for retraining, the proposed regulations require that it be provided to all members of the workforce who have access to protected health information, as relevant to their function within the entity, whenever privacy policies and procedures materially change.26

Understand who has access to what information

Thus, training is likely to be an ongoing challenge. Beyond the issues of designing initial training which is relevant to the particular functions of each workforce member with access to protected health information, it will be necessary to understand which workforce 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 access to protected health information and, if so, the nature of that job’s involvement in using, handling, or disclosing that information. Compiling this information will be tedious at best, and larger organizations will find the task daunting but necessary. A useful strategy for accomplishing this would be to inventory all existing software applications and their data content. For those applications involving protected health information, a list of all users should be compiled, analyzing their data access needs. There are several supplementary 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, job descriptions may not exist for all members of the workforce, as defined by the proposed regulations. According to the proposed regulations, “workforce” means employees, volunteers, trainees, and other persons under the direct control of a covered entity, including persons providing labor on an unpaid basis.27 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, e.g., for volunteers. In some cases, it may be necessary to conduct workforce interviews or to observe work being performed to fully understand the level and breadth of access to information.

This “information access inventory” will need to be kept 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 workforce will require retraining.

Consider other likely functions for the privacy officer

Beyond these required and implied duties, a number of other important functions may fit well within the responsibilities of the privacy officer, depending upon their particular skill set. Reviewing and negotiating business partner contracts to bring them into compliance with the final privacy rules will be a large 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 164.506(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.
Another responsibility for the privacy officer is likely to be 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. Being the most knowledgeable internal contact, the privacy officer will likely be heavily involved in any investigations.

In addition, 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, in accordance with the regulations. 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 be familiar with applicable HIPAA requirements.

It may also be wise to consider administratively grouping, insofar as feasible, key information-handling departments and functions under (or alongside of) 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. 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:

- 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 procedures areas
- Admitting/Patient Registration
- Patient Accounting/Finance
- Home Care Program
- Hospice Program
- Volunteer Department

And these are only the likeliest candidates. Don’t forget about departments who can be expected to have access to health information, even though their jobs don’t require them to use that information, such as is true with Housekeeping/Environmental Services staff who empty trash containers that may contain protected health information. Indeed, it may be simpler to list those departments without likely access to protected health information.

In any event, there may be efficiencies gained from grouping key information-handling departments, such as Health Information Management, Information Services, Quality Improvement, and the like, under (or with) the privacy officer to foster communication on HIPAA-related issues.

To whom should the privacy officer report? Although the final decision will be a function of each organization’s culture and the players involved, there are many arguments in favor of placing the privacy officer at a high level within the organization (i.e., reporting to the CEO, COO, CFO, General Counsel, or CIO):
• The privacy officer will be involved in organization-wide changes to policies, procedures, and training, and ensuring compliance with the required changes will demand a high level of authority;

• Success in the position will require close working relationships with the organization’s leadership (administration, medical staff, board of directors, legal counsel, and department heads);

• The broad skill and knowledge requirements of the position demand a relatively high-level candidate, who will likely expect high-level placement within the organizational structure.

What non-healthcare models might add to our game plan

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 appears to be “yes.” Outside of healthcare, an increasing number of companies have turned to a new corporate player, often called chief privacy officer (CPO), to prevent legal and/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 of these 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 suit. “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,” said Ward Hanson, a lecturer at Stanford’s Graduate School of Business. “So smart companies will have these skills in-house and will invest the resources necessary to make it an important function.”

In most published models, the CPO reports to the CIO or CEO. The job requires a certain amount of fortitude and high-level authority for the potential CPO candidate. “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. “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.’”

McGraw-Hill Companies has taken a hybrid approach, by combining privacy officials at the business unit level, with a corporate-wide steering committee of senior executives. CEO Harold McGraw III has described their five-step approach to privacy compliance:

1. Oversight: A Customer Privacy Steering Committee, comprising senior business and corporate executives, meets regularly to ensure that privacy policies and issues receive high-level attention.

2. Review: The corporate audit department coordinates periodic random reviews of actual compliance with existing policies. Evidence of failure to comply is pushed up to senior management so that changes can be made to bring the offending business unit into compliance.

3. Ethics: McGraw-Hill has expanded their Code of Business Ethics to include a commitment to comply with their privacy policy, and to trigger disciplinary actions in cases involving violations of that policy.

4. Contact Points: Each business unit has a designated Privacy Official: someone customers can contact to raise privacy concerns, and get those concerns resolved.

5. Reporting: After a year’s experience with their policy, McGraw-Hill has posted their policy on their website. They also make it available in an annually printed “business privacy report”. This report tells customers about the organization’s commitment to the privacy policy, their progress in implementing it, and any changes made over the past year in that policy.

There are, however, some potential downsides to designating anyone solely as a privacy officer—and having that be their only job function, says Julia Johnson, privacy coordinator for Bank One Corp. One risk is that doing so might let all other parts of an organization feel that they had been let off the hook. That is why she decided not to have a privacy staff under her. If she did, people might think Johnson’s office was where the privacy buck should always stop. She views her role more along the lines of a missionary’s. “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,” explains Johnson. “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.”
WHO ARE THE LIKELY CANDIDATES FOR PRIVACY OFFICER?

Once we’ve roughly defined the potential scope and duties of our privacy officer, we need to determine the skill set required—and whether we can find this skill set within existing staff. Corporations hiring Chief Privacy Officers have struggled with this question as well.

Obviously, the healthcare organization’s needs for a privacy officer will be slightly different than non-healthcare businesses, because HIPAA provides a framework we will have to work within. Nevertheless, an understanding of applicable laws, a sensitivity to public relations, and at least a basic understanding of information technology seems fundamental. Here are a few of the skills (in no specific order) 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, inspectors
- Understanding of information technology
- Expertise in reviewing (and potentially drafting) contract language
- Ability to promote what may be “unpopular” positions and policies.

Where do we find people with these skill sets? Several positions within a typical healthcare organization have some (if not all) of these skills:

- Health information managers;
- In-house counsel;
- Risk managers;
- Directors of compliance;
- Directors of medical affairs;
- Information systems managers, and
- Administrators over these functional areas.

WHAT RESOURCES EXIST FOR THE PRIVACY OFFICER?

Regardless of their background, the privacy officer is likely to need the assistance of other subject matter experts within your organization, such as those positions listed above. It may be useful to form an ad hoc privacy council that can offer advice and support to the work of the privacy officer, 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, took that information and has begun working towards compliance.34

Fortunately, numerous resources are available to assist the new privacy officer, and many of them are free or very low cost.

A plethora of websites offer HIPAA-related information, checklists, and other resources. Healthcare publishers and associations have also delivered a wealth of articles, checklists and practice briefs to assist in privacy-related compliance efforts. A small sampling of free or low-cost resources can be found in the handouts for this session.

HOW WILL WE MEASURE SUCCESS?

Appointing a privacy officer and simply hoping for the best won’t get us where we need to go. The importance of this position warrants setting performance measures and benchmarks if we are to
achieve real benefits in improving privacy and confidentiality in our organizations — benefits that accrue as much to the healthcare organization as to its patients.

What potential performance measures can we use and track, over time, to evaluate our success?

• 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 workforce members receiving privacy training on time (according to mandated schedules)
• Percentage of workforce with current privacy/confidentiality certifications on file
• Accrediting agency citations involving privacy/confidentiality.

HIPAA presents us with many new challenges, and as many opportunities. The privacy officer will play a key role in contributing to our success— or our 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.

AUTHOR BIOGRAPHY

Jill Callahan Dennis is principal of Health Risk Advantage, a Denver-based risk management consulting firm. She is author of “Privacy and Confidentiality of Health Information”, published September 2000.

REFERENCES

1 See section 164.518(a)(1) of the proposed Privacy Rule, and section 164.520(c)(2).
2 HIPAA’s civil monetary penalties are detailed in Section 1176 of the Health Insurance Portability and Accountability Act; the criminal penalties for “knowing” misuses or disclosures can be found in Section 1177.
3 See section 164.518(a)(2) and section 164.520(c)(2) of the proposed rule.
4 See section 164.506(b)(2)(i) and section 164.520(c)(3).
5 See section 164.506(b)(2)(ii) and section 164.520(c)(3).
6 Section 164.5506(b)(2)(i) and section 164.520(c)(3).
7 Section 164.506(c)(2)(i) and section 164.520(c)(3).
8 Section 164.506(c)(2)(ii).
9 Section 164.506(c)(2)(iii).
10 Section 164.506(c)(2)(iv), and 164.520(c)(1)(ii)(A) and (B).
11 The need for these procedures are implied, but not explicitly required, by section 164.508(a).
12 The need for documented policies and procedures is implied, but not explicitly required, by sections 164.508(b)--(e).
13 The need for documented policies and procedures in situations where authorization is not required is implied, but not explicitly required, by section 164.510.
14 The need for written procedures is implied, but not explicitly required, by section 164.512. They are, however, required by section 164.520(d)(1) and 164.520(d)(8).
15 These procedures are required by section 164.514(c) and (d), section 164.520(d)(2-4), and section 164.520(d)(8).
16 Disclosure accounting procedures are required by section 164.515(b) and (c), and also by section 164.520(d)(5) and (8).
17 See section 164.516(b)--(e), section 164.520(d)(6-7), and section 164.520(d)(8).
18 The need for written procedures on training is implied, but not explicitly required, by section 164.518(b). It is, however, required by section 164.520(e)(2).
19 See section 164.518(c)(2).
20 See section 164.518(d)(1) and (2), and section 164.520(e)(4).
21 These policies and procedures are implied, but not explicitly required, by section 164.518(e).
    They are, however, required by section 164.520(e)(5).
22 See section 164.518(f) and section 164.520(e)(6).
23 See section 164.520(e)(3).
24 Record retention policies are implied by section 164.520(f).
25 Training requirements are addressed in section 164.518(b).
26 See section 164.518(b)(2)(i)(A) and (B).
27 See section 164.518(b)(2)(ii) and (iii).
28 See section 164.518(b)(2)(iv).
29 “Workforce” is defined in section 164.504.
30 Margaret Steen and Elise Ackerman, “Companies Hiring Chief Privacy Officer,”
31 Kosan, Lisa, “E-biz execs guard Net privacy—CPOs oversee companies’ personal data policies,”
    eWeek, August 14, 2000, p. 60.
33 Cocheo, Steve, “Making privacy a brand issue at Bank One,” ABA Banking Journal, July 2000,
    p. 20.
35 Fuller, Sandra, A Setting the Foundation for Compliance through Effective Policies,”
    presentation at 2000 HIPAA Conference of the Joint Healthcare Information Technology