

Finger on the Panic Button?

Don't Worry: Here Are the Basic Steps to HIPAA Compliance



by Annette Miller, JD
Chief Compliance Officer, Attorney
HIPAAAnswers
Eden Prairie, MN

It is a little more than a month to go before small health plans, the final group affected by HIPAA, must be in compliance with the HIPAA Privacy Regulation. As the April 14th deadline nears, many will be in panic mode and have no idea where to even start.

If you are just beginning the HIPAA compliance process, conducting your annual HIPAA privacy audit, or are a business associate trying to become HIPAA-compliant, follow these steps to make the process smoother.

Step 1: Put Someone in Charge of the Project

Appoint a Privacy Official who can manage the HIPAA compliance project from beginning to end. The Privacy Official is responsible for the development and implementation of the privacy policies and procedures for the organization. This individual must have a thorough understanding of state and federal laws governing the use and disclosure of protected health information (PHI). In addition, the individual should be aware of the consequences for failure to comply with the HIPAA regulations.

The Privacy Official must ensure management has a basic understanding of such laws. Appointing this individual is required under the HIPAA privacy regulation

and doing it now will allow you to check off the first HIPAA requirement.

Step 2: Determine What Type of Organization You Are

You need to understand your organizational structure. Are you a single corporation or does your organization have multiple subsidiaries? Do you operate in multiple locations or states? This is important in determining whether the organization will elect itself as a *hybrid entity* or an *affiliated entity*.

Why is this type of election important? Affiliated covered entities are treated as one single covered entity for HIPAA purposes. The advantages of affiliate entities:

one Notice of Privacy Practices, one Privacy Official and one authorization.

If an organization elects itself as a hybrid entity, then appropriate “firewalls” will need to be implemented between departments to ensure no PHI is shared. An example of a hybrid entity is an employer that wants to maintain information about its covered group health plans from the non-covered group health plans (e.g., workers’ compensation or disability plans). A disadvantage of not electing to be a hybrid entity is that the HIPAA requirements may need to be implemented for the entire organization.

Step 3: Identify the Types of Group Health Plans Covered

Identify the group health plans that the organization offers to its employees. Medical plans, dental plans, vision plans, FSAs, prescription plans, certain employee-assistance programs and on-site clinics are all considered to be types of health plans covered under HIPAA. For each health plan ask these questions: Is the plan insured or self-funded? *Is there a single plan or multiple plans? Does the employer rely on an insurer to handle day-to-day operations of the plan? Does the employer use a third-party administrator? Are there other types of plans (e.g., disability, workers’ compensation) that the employer is trying to integrate with the health plan?*

For each of the group health plans, you will need to determine the number of participants and whether they are self-administered by the health plan. In other words, does the organization manage the entire administration of the plan in-house? If the plan is self-administered with fewer than 50 participants, the plan is exempt from HIPAA compliance. In addition, workers’ compensation, life insurance, accident only and disability insurance benefits are not considered covered health plans under HIPAA unless the organization is trying to integrate with a covered health plan or information is maintained in one file or integrated benefits system.

Step 4: Identify the Flow of PHI in the Organization

This step will require you to conduct an inventory of PHI in your organization. PHI is information created or received by a provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health condition of an individual or payment of health care to an individual.

The following checklist should assist your organization in identifying PHI. Ask if your organization handles PHI in any of the following ways or purposes:

- ✓ Exchange PHI with outside entities (insurance companies, TPAs, clearinghouses, health care providers, insurance brokers, etc.)?
- ✓ Create, maintain, modify, edit or review PHI any form (e.g., oral, paper or electronic)?

- ✓ Transfer or receive PHI with other departments within your organization?
- ✓ Use or disclose summary or “de-identified” health information?
- ✓ Use or disclose PHI in connection with any other benefit plan of the plan sponsor (e.g., LTD, STD or workers’ compensation)?
- ✓ Use or disclose PHI in connection with utilization review, risk or compliance audits, quality assessment and improvement studies, business planning, fundraising, marketing, claims review or disease and case management?
- ✓ Use or disclose PHI for any other business or health care activity?

After identifying PHI in the organization, ask:

- ✓ Who within the organization receives the PHI?
- ✓ To whom is it disclosed?
- ✓ How is it used/disclosed (e.g. phone, fax, mail, email)?
- ✓ For what purpose is it received/used/disclosed?
- ✓ Where is PHI retained within your organization physically (e.g., file cabinet, computer file, etc.)?

Once finished, save this PHI inventory list. It will help you comply with the Security Regulation.

Step 5: Identify Your Business Associates

You must identify the business associates that work on the behalf of the covered entity. Examples of business associates are brokers, agents, lawyers, accountants, utilization review companies or third-party administrators. Here is a simple analysis for you to use in determining if a vendor is a business associate.

? Does the vendor perform or assist in the performance of a function or activity involving the use of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing benefit management, practice management and repricing, on behalf of the Covered Entity? If yes, the vendor is a business associate.

? Does the vendor perform or assist in the performance of such a function as a member of the Covered Entity’s workforce? If yes, the vendor is NOT a business associate.

? Does the vendor provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for the Covered Entity, where the provision of the services involves the disclosure of individually identifiable health information from the Covered Entity or from another business associate of the Covered Entity? If yes, the vendor is a business associate.

Information may be shared with a lot of people who are not performing services on behalf of the organization. These people are not business associates. Determine who the information is going to and, if they are not business



associates, determine why they may be entitled to the PHI. You may need to obtain confidentiality agreements with these vendors or obtain appropriate authorizations before releasing information to them. Remember, the organization must have written contracts in place with all business associates no later than April 14.

Step 6: Draft and Implement the Policies & Procedures and Forms

By now you should have a clear understanding of your organization and how it handles protected health information. You are now ready to begin drafting the policies and procedures.

Begin by identifying the privacy requirements applicable to your organization. Second, determine what will need to be drafted (e.g., policy, procedure, form or contracts). Draft your policies, procedures and forms to meet the HIPAA regulatory requirements. A service like HIPAAAnswers can help significantly by having template policies, procedures and forms for you to customize based on the information you have gathered about your organization. In addition, our service will tell you the requirements applicable to your organization.

In addition to complying with the HIPAA regulations, you will also need to ensure that the organization is complying with current state law. Remember, HIPAA creates a “federal floor” for protection of information and, generally, HIPAA regulations will apply. However, there are few exceptions where your state law must be followed.

One important point exception is that if a state’s law is more protective of an individual’s information, the state law will override HIPAA. When reading the state law, keep in mind the differences between “must” and “may.” HIPAA may allow certain disclosures, but if state law does not permit the disclosure, state law will apply and the disclosure is not permitted.

Once the drafting has been completed, you are ready to begin implementing the documents within your organization.

Step 7: Train Your Workforce

It is not enough to simply draft your policies, procedures and forms and put them on the bookshelf. HIPAA requires that implement them in your organization and train your staff on the documents in order for employees to carry out their job functions. The training requirement is ongoing. Also, the organization must train all new employees within a reasonable time after they join the organization. In addition, staff must be trained (again, within a reasonable period of time) if there are any material changes in the policies, procedures or forms.

One important point exception is that if a state’s law is more protective of an individual’s information, the state law will override HIPAA.

Step 8: Update the Documentation

Finally, your organization needs to have a system in place to monitor changes in the HIPAA regulations and state laws. Just like the training, the HIPAA compliance process will be ongoing. HIPAA requires you to update your policies, procedures and forms when there are changes in the HIPAA regulations, state laws or your business practices. Therefore, at a minimum, your organization should re-evaluate its policies and procedures on an annual basis to ensure it meets the regulatory requirements and that employees are complying with the procedures. ■

Annette Miller has more than 15 years of experience in the health insurance industry. She graduated cum laude from William Mitchell College of Law and holds a master’s degree in public administration, with a minor in health care administration, from Drake University. She can be reached at Annette_Miller@hipaanswers.com or 952-400-1100.