

# Steps to HIPAA Security Compliance

*By Annette Miller, J.D.*

*HIPAAAnswers™*

*Vice President of Compliance Services/Corporate Counsel*

As the April 21, 2005 security compliance date gets closer, many employer sponsored health plans and providers are asking where do they begin. While the deadline may seem a long ways off, there is an abundance of work a head to meet the security requirements. So where do you start? I recommend that you follow these steps.

## **Step 1: Appointing someone in charge of the project**

First, appoint the Security Official who can manage the HIPAA security compliance project from beginning to end. The Security Official is responsible for the development and implementation of the security policies and procedures for the organization. This individual must have a thorough understanding of state and federal laws governing the use and disclosure of electronic protected health information (EPHI). In addition, the individual should be aware of the consequences for failure to comply with the HIPAA regulations. Appointing this individual is required under the HIPAA security regulation and doing it now will allow you to check off the first HIPAA requirement!

## **Step 2: Determine the type of your organization**

Second, 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 are the affiliate entities have one set of security policies and procedures to be followed by all the entities. If an organization elects itself as a hybrid entity, then appropriate “firewalls” will need to be implemented between the departments and employees handling electronic protected health information (EPHI) from the rest of the organization to ensure no EPHI is shared. An example of a hybrid entity is an employer who wants to maintain information about their covered group health plans from the non-covered group health plans (e.g. workers compensation, disability plans). A disadvantage of not electing to be a hybrid entity is that the security policies and procedures will have to be implemented for the entire organization.

## **Step 3: Identify the Flow of EPHI in the organization**

This step will require you to conduct an inventory of EPHI in your organization. The following checklist should assist your organization in identifying PHI:

HIPAAAnswers™ 8941 Aztec Drive, Eden Prairie, Minnesota 55347

866.326.6785

[www.HIPAAAnswers.com](http://www.HIPAAAnswers.com)

1) Does your organization handle EPHI in any of the following ways or purposes:

- Exchange EPHI with outside entities (insurance companies, third party administrators, clearinghouses, health care providers, insurance brokers, etc....)
- Create, maintain, modify, edit or review EPHI.
- Transfer or receive EPHI with other departments within your organization.
- Use or disclose summary or de-identified electronic health information.
- Use or disclose EPHI in connection with any other benefit plan of the plan sponsor (e.g. long term disability plan, short term disability plan, workers compensation).
- Utilization review
- Risk or compliance audits
- Quality assessment and improvement studies
- Business planning
- Fundraising
- Marketing
- Claims review
- Disease and case management
- Use or disclose EPHI for any other business or health care activity

2) After identifying EPHI in the organization, ask the following questions:

- Who within the organization receives the PHI?
- To who is it disclosed?
- How is it used/disclosed (e.g. phone, fax, mail, email, electronic, etc...).
- For what purpose is it received/used/disclosed?

- Where is it retained within your organization physically (e.g. hard drive, computer file, disks, CDs, etc...)?

(3). Create an inventory of all of your hardware, software and other media.

#### **Step 4: Identify your Business Associates**

Fourth, you must identify the business associates that work on your organization's behalf. Examples of business associates are brokers, agents, lawyers, accountants, utilization review companies or third party administrators.

EPHI may not be created, used, disclosed or shared with the business associates until there is a business associate contract put in place. The business associate must agree to put appropriate administrative, physical and technical safeguards in place. In addition, the business associate must assure that any agents or subcontractors they use in performing their services also have appropriate security safeguards in place. Finally, you and the business associate need to develop a process in which any security breaches or incidents are reported to your organization. Remember, the organization must have written contracts in place with all business associates by no later than April 21, 2005 containing the new security contract requirements.

#### **Step 5: Conduct a Risk Analysis**

This is the most important step your organization will complete in the security compliance process. During this step you will be reviewing your computer systems, physical security around your office and the computer systems, reviewing existing policies and procedures, evaluating your disaster recovery plans, backup plans and determining your employee's awareness of security. Taking the inventory you created in step 3 above, you will be evaluating each computer system to determine how critical it is to your business, what the risks are associated with each computer system, what security controls you currently have in place and what security controls need to be implemented.

#### **Step 6: Draft and Implement the policies and procedures and forms**

By now you should have a clear understanding of your organization and how it handles EPHI. You are now ready to begin drafting the policies and procedures. Determine what will need to be drafted (e.g. policy, procedure, form or contracts) and what documents that will need to be amended. HIPAAAnswers™ can help significantly since we provide 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 security requirements applicable to your organization.

In addition to complying with the HIPAA Security 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. Therefore, you must also be aware

of your state laws and comply with those state laws that are more stringent or stricter than HIPAA. Once again, HIPAAAnswers™ can provide you with the state laws.

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 you to train your staff on the documents in order for the employees to carry out their job functions. Under the Security Regulation, you are also required to train all of your management staff. The training requirement is on-going. This means you must have a procedure in place to train all new employees, employees that switch jobs within the organization. In addition, employees must be trained if there are any material changes in the policies, procedures or forms. Consider training your staff on a regular basis (at a minimum annually) to ensure that the security of EPHI in your organization is taken seriously and your policies and procedures are being followed.

### **Step 8: Update the Documentation**

Just like the training, the HIPAA compliance process will be on-going. HIPAA Security Regulation requires you to review your policies, procedures and forms when there are operational or environmental changes or changes in federal or state laws. Therefore, your organization should review its policies and procedures on at least an annual basis.

*Annette Miller is the Vice President of Compliance Services/Corporate Counsel for HIPAAAnswers™. She has over 15 years experience in the health insurance industry. Annette graduated from William Mitchell College of Law, cum laude and holds a masters degree in public administration with a minor in health care administration from Drake University. She can be reached at [Annette\\_Miller@hipaanswers.com](mailto:Annette_Miller@hipaanswers.com) or 952-400-1100.*