

## **HIPAA for Employers and Health Plan Sponsors**

### **What does HIPAA mean to an employer?**

**HIPAA presents an interesting set of issues** for an employer that sponsors a health care plan. There three basic questions to ask if you are an employer with a medical plan that covers your employees.

1. The first question is do you as an employer have to deal with HIPAA at all.
2. Secondly, if your healthcare plan does have to be HIPAA compliant to what degree must you as an employer also have to be compliant?
3. And what does HIPAA compliant mean anyway.

**Let's deal with the first question**, is your health plan a covered entity and what does that mean? HIPAA defines healthcare plans as covered entities that have::

1. 50 or more eligible participants OR
2. Has a third party involved with the administration, such as a Flexible Spending Account (FSA) or an Employee Assistance Program (EAP).

**Covered entities must be HIPAA compliant.** Before we discuss what compliant means, let's talk about what 50 more participants means. HIPAA uses a different definition than Cobra does. Cobra refers to number of employees. HIPAA focuses on *participants* in the plan. There is no specific definition of participants. An accepted interpretation is to think of eligible employees. If you have 75 employees and all are eligible, including Cobra participants, but only 45 are taking medical coverage, you should consider your plan to be over 50 participants. It is always better to err on the conservative side.

**Notice the criteria said nothing** about whether the employer actually received the medical applications only the number of eligible employees OR whether a third party is involved in the plan administration such as an FSA (Flexible Spending Account.) How your company handles the applications is something you do as a covered entity and that goes into your Policies and Procedures Manual.

**So HIPAA says your healthcare plan is a covered entity.** Covered entities must be HIPAA compliant. Where does an employer fit in the HIPAA picture. It would have been much easier if the HIPAA regulations would have made the employer a covered entity instead of a plan sponsor. But it didn't. As a plan sponsor, an employer has responsibilities similar to a Business Associate. An employer must "sign" an agreement with the covered entity/healthcare plan agreeing to protect employee health information used in the administration of the medical plan. But the responsibility is somewhat deeper since the employer is more than a sponsor of a healthcare plan.

1. Without the employer, there is no healthcare plan and
2. The healthcare plan does not have employees to carry out the HIPAA compliance efforts, therefore the employer must do it.

*So a healthcare plan cannot itself be compliant. It is the employer as Plan Sponsor that must carry out the steps.*

## **What does it mean to be HIPAA compliant?**

**First, let's review** another area concerning the employer. If your healthcare plan is a covered entity to what level must you as an employer be involved? We feel that its a matter of what is the degree of compliance rather than asking if you need to be at all. All "plan sponsors" must have a HIPAA Policies and Procedures Manual. This manual must spell out what your HIPAA Policies and Procedures are. Even if you determine as a plan sponsor your HIPAA requirements are minimal, you must have a HIPAA Manual saying what they are and how things are handled.

**A key point** here is how do you as an employer receive the "protected health information." Interesting enough, information used to apply for a job is not PHI (protected health information) where the same information used to apply for medical insurance is PHI. (i.e.: an employee social security number, or home address or medical history). We will address this specific issue later.

**The next point** is to what level is the employer involved with the healthcare plan administration and the employee PHI. Here are some examples to illustrate different levels of involvement.

1. *An employer that has chosen to self insure* the medical plan, using a TPA (Third Party Administrator) with stop loss insurance, claims administration and so forth is about as deep in the HIPAA compliance water as an employer can get. The employer is considered to be part of the process and by definition has access to claims and employee medical history, conditions, etc. Full compliance is required.
2. *An employer that purchases a fully insured medical plan* (or some hybrid self insured or minimum premium type of plan) that includes a HRA (Health Reimbursement Account), HSA (Health Savings Account), Medical Savings Account (MSA) or offers a FSA (Flexible Spending Account) or Employee Assistance Program or any or all of the above is not as deep as the prior example but pretty deep in the HIPAA water. These types of plans require some type of administration of the claims reimbursement for employees. The employee turns the EOB (Explanation of Benefits) in to someone for reimbursement. This is PHI and must be protected. Having a third party administrator handle the claims *does not remove* the employer from HIPAA compliance necessity. By the way, a TPA would be a Business Associate of the Healthcare Plan and must also sign an agreement. And while we are talking about third party Business Associates, so is the insurance broker.
3. *An employer obtains a fully insured medical plan* from an insurance company. The employer does not deal with the employee medical applications AT ALL, a third party does in some way. The FSA/HRA is handled directly by a third party that recognizes HIPAA and keeps the employer and administration employees

away from the PHI. This employer has minimal HIPAA exposure. Note I said minimal. HIPAA still requires a Policies and Procedures Manual explaining that is how the plan is administered. This is a good reason to use third parties to do many of the duties of a healthcare plan rather than manage it internally.

4. *The only exception* for a healthcare plan is one that:
  1. *Has fewer than 50 participants,*
  2. *Is fully insured* by an insurance company
  3. *AND does all other administration for the plan internally.* That means if there is a Flexible Spending Account it is administered by the employer and *not a third party.*

**Rest assured,** healthcare insurance companies, HMO's, third party administrators, Flex companies and most insurance brokers are very aware of HIPAA requirements. Most if not all of them are implementing procedures to protect their clients (employers like you) as much as they can. These people cannot take the HIPAA requirements away from your healthcare plan, but they can minimize your exposure.

**We think, as a plan sponsor,** your company should implement HIPAA policies and procedures regardless of your specific hows and whys of PHI and HIPAA. We think that as broad as the law is, and the fact it overlaps with other state and federal privacy requirements, it is a good business practice to implement HIPAA compliance. Consider the following points:

1. It is possible to minimize an employer's HIPAA exposure but you *cannot eliminate it.* If your company is a plan sponsor, you have HIPAA compliance issues to deal with.
2. Can you guarantee that you and your employees will never receive PHI from the administration of the healthcare plan? Or that copies of employee medical applications will never be seen by an administration employee or copied to an employee file?
3. As an employer you receive data that could be considered PHI depending on how and why you get it such as a sick leave requirements or FMLA situation or you have a health nurse on staff, or an health emergency at work, and so on. Will your employees to know when the information is PHI and when it is not?
4. Will the third parties that handle the administration of your Flex Plan or HRA always keep PHI away from your company? Having a third party do functions for

your healthcare plan does not take away your HIPAA responsibilities only delegates them to someone functioning *as an agent to your healthcare plan*.

5. Any form of self insurance will create broader HIPAA compliance issues, such as an HRA, MSA, HSA and even a Flex Plan. HRA's, HSA's and partial self insurance can be an attractive method of providing medical insurance for employees if not today, perhaps tomorrow, considering the increasing cost of medical coverage.

**We think that HIPAA compliance should be applied** across the board also when it comes to employee information. It does not make sense to only protect it under certain circumstances. The requirements of HIPAA really aren't much more than what your company should be doing anyway under other state & federal privacy laws and common sense. The security aspects of HIPAA are things ALL employers should be doing regardless of HIPAA.

**ER.HIPAAps.com site takes the conservative approach** to HIPAA compliance. It is very complicated to attempt to determine whether this or that HIPAA requirement applies to each plan sponsor. Rather than waste time and money going through an complicated analysis, arguing whether you can skip this requirement or have to do that one, we recommend a more conservative approach. What should be done to protect your company from a costly and time consuming HIPAA audit? Use our website to follow the steps to create a HIPAA Policies and Procedures Manual.

**HIPAA requirements are pretty straight forward** for an employer. Below are the main points to HIPAA compliance.

1. Designate a *privacy officer* who job it is to develop and implement HIPAA policies and procedures
2. *Identify employees* or classes of employees who will have access to PHI and under what circumstances this access will be permitted
3. *Develop a privacy training program* for your healthcare administration employees
4. Document all administrative measures and how PHI is to be used and protected including employee sanctions for non-compliance. (*Policies and Procedures Manual*)
5. Furnish participants with a *written notice of the plan's policies* regarding the privacy of and access to PHI. (*Notice of Privacy Practices*)
6. Create several forms including reports, employee authorization, complaint and documentation for non-compliance actions
7. Obtain *Business Associate Agreements* from third parties involved with the administration of your healthcare plan
8. Develop security procedures to protect any protected information from internal and external access

**ER.HIPAAps.com will assist you in this process.** When you have completed our steps, you will have a HIPAA Policies and Procedures Manual that outlines (and recommends) actions to take. When you have completed the Manual selections, a tool will be available to train any employees involved with the healthcare plan administration. There also is a library of examples to use to create your own forms with your legal counsel's input.

**One last thought**, when we were creating a HIPAA tool for employers, we approached it very conservatively. We asked what would an employer need as a healthcare plan sponsor to defend a challenge to HIPAA compliance. From there we worked backwards to build a tool for you to use to create your HIPAA Manual.

Dennis P. Begley CLU ChFC  
ER.HIPAAps.com