EMPLOYERS AND THEIR
Self-insured Health Plans

1. What is the relationship between an employer and its self-insured health plan?

It's a delicate one. Typically, an employer will sponsor (i.e., go through the legal formalities) necessary to establish a health plan for its employees. To the casual observer, the plan will look like nothing more than a piece of paper. The plan itself often will have no assets of its own – the employer pays all claims directly out of its general accounts; it has no offices; all contracts with third parties for services needed to operate the plan (e.g., TPA services) are with the employer who also pays the fees for those services; and the plan has no employees of its own – any in-house work needed to operate the plan is performed by employees of the employer.

As a consequence, it is common for an employer to think of its health plan as little more than an extension of itself, a department or cubicle within the company where the health plan is administered.

In fact, the health plan is, in essence, a legal entity separate and distinct from the sponsoring employer. For example, a plan could, in fact, have assets, offices, contracts and employees of its own. An employer that fails to observe the distinction between itself and its plan, runs the risk of violating HIPAA's privacy requirements.

2. What is the most common consequence of an employer's failure to observe the distinction between itself and its plan?

Based on our experience, employers tend to think that Protected Health Information (PHI) in the possession of the plan is generally available to the employer. This is particularly tempting where an employer does in fact perform certain plan administration functions that do require access to PHI. As a consequence, we see employers seeking to obtain and use PHI in ways that are inconsistent with HIPAA.

3. Are you saying that an employer can never get PHI about its employees?

No; however, in order to obtain PHI, the employer must impose, implement and observe certain formal and functional requirements.

4. What formal and functional requirements must an employer follow to obtain and use PHI?)

We'll start with formal requirements.

In order to receive PHI from its plan, an employer makes sure that its plan documents:

- Set out the permitted and required uses and disclosures of PHI, which must be limited to plan administration functions actually performed by the employer.
- Require the employer to certify to the plan that it will comply with the following provisions, which the employer has included in the plan documents. They provide that the employer will:
  - Not use or further disclose the information other than as permitted or required by the plan documents or as required by law;

- Ensure that any agents to whom it provides protected health information received from the group health plan agree to the same restrictions and conditions that apply to the plan sponsor with respect to such information;
- Not use or disclose the information for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the plan sponsor;
- Report to the group health plan any use or disclosure of the information that is inconsistent with the uses or disclosures provided for of which it becomes aware;
- Make available protected health information for amendment and incorporate any amendments to protected health information; and make available the information required to provide an accounting of disclosures, all in accordance with the requirements of the privacy rule;
- Make its internal practices, books, and records relating to the use and disclosure of protected health information received from the group health plan available to the Secretary of Health and Human Services for purposes of determining compliance by the group health plan with the privacy rule;
- If feasible, return or destroy all protected health information received from the group health plan that the employer still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and
- Ensure that adequate separation is established between the plan and the employer as described in more detail in the next bullet point.

» Provide for adequate separation between the employer and its health plan by:

- Describing those employees or classes of employees or other persons under the control of the employer to be given access to the protected health information to be disclosed. This must include any employee or person who receives protected health information relating to payment, under health care operations of, or other matters pertaining to the group health plan in the ordinary course of business;
- Restricting the access to and use by such employees to the plan administration functions that the plan sponsor performs for the group health plan; and
- Providing an effective mechanism for resolving any issues of noncompliance with the required plan document provisions.

5. That's quite a list. It talks a lot about limiting employer access to "plan administration functions." What are they?

For purposes of this topic, plan administration functions include those needed to pay claims, determine eligibility, obtain employee contributions, handle appeals, obtain stop-loss coverage and conduct quality assessment and improvement activities. Keep in mind that even if an employer properly gets PHI for a plan-related function, it cannot use it for any other purpose.

6. So does this mean that an employer can get claims data on its employees and their dependents?

Not necessarily. Remember that in addition to limiting access to plan administration functions, the function in question must be identified in the plan documents as one the employer actually performs. For example, while there is no rule that says an employer can't administer and pay claims incurred

under its plan, most employers hire a third party administrator to handle that task. In those cases, the employer would not be permitted the same type of detailed access to PHI that the TPA would have. Similarly, many employers use a broker to place stop loss coverage. As such, the broker might need PHI on the high dollar cases that would be of interest to a potential carrier, but the employer might not. Another common example is claim audits. Here too, most employers will hire an audit specialist and while the employer certainly has an interest in knowing whether its TPA's financial accuracy is 90% or 99.9%, it probably does not need information about specific claims.

7. What about situations where the employer does need to get PHI for some plan administration function that it has retained?

In that case, the employer can get the PHI it needs subject to the "minimum necessary" restrictions in the privacy rule.

8. What are the "minimum necessary" restrictions in the privacy rule?

When a plan provides PHI to an employer, it must limit the amount of PHI to just what is necessary for the employer to perform the function for which it is requested. There are no hard and fast rules that govern the application of the minimum necessary standard (although the government has promised future guidance in this area.) As it stands, plans and employers must use a reasonableness standard in deciding what is minimally necessary.

For example, some employers retain the right to decide appeals of denied claims. Imagine a claim that has been denied on the grounds that the treatment was not medically necessary. In order to resolve an appeal of that claim, the employer is probably going to need a lot of detail about the individual's condition. However, one thing that the employer may not need to know is the name of the person involved since the decision on appeal should be the same regardless of the person's name.

Conversely, suppose a claim has been denied on the grounds that a person is not an eligible dependent. In order to resolve that appeal, the employer may need the names of the employee and dependent involved but should not need any information about the nature of the claim itself.

9. Is it a problem if an employer insists on having copies of all EOBs so that they can assist employees with questions about their claims?

There are two major problems with this. The first is that assisting employees with claims questions is not a plan administration function (the employer is working on behalf of the employee not the plan). Even if that were not the case, the employer would not need routine access to PHI on all employees just to help the few who request assistance.

10. Can you give examples of other situations where an employer may or may not be able to get PHI without a release from the individual?

This is by no means a comprehensive list; and keep in mind that even in those situation where PHI is available to the employer, the minimum necessary restrictions still apply.

- If an employee is submitting fraudulent claims, the employer may be able to get the PHI needed to take appropriate action to recover improperly paid benefits and, if the plan permits, terminate coverage. However, the employer could not use the information to otherwise discipline the employee because that would be an HR function, not a plan administration function.
- An employer may not use or disclose PHI from its health plan in connection with the administration of its disability plan or any other benefit plan.

- An employer may need PHI from its wellness plan in order to administer a health plan-related incentive program. However, employers should carefully think through the application of the minimum necessary rule. For example, in a typical case, an employer will hire an independent third party to conduct wellness screenings. Does the employer need to know the actual results of the screening or is it sufficient that the third party just report the names of the individuals who met the wellness plan standards?
- An employer may obtain PHI from its health plan to the extent it is needed in connection with a merger or sale of the company.

11. What operational requirements are imposed on an employer with a self-insured health plan?

HIPAA imposes a number of administrative or operational requirements on health plans. Those requirements do not apply directly to the sponsoring employer; however, in the typical case where the plan itself has no employees, in practice all plan administrative functions are performed by third parties (generally the employer) and so the employer is responsible for effecting the plan's compliance with these requirements.

The requirements include the following:

- The appointment of a privacy officer who is responsible for the development and implementation of the policies and procedures of the plan.
- The designation a contact person or office who is responsible for receiving complaints under this section and who is able to provide further information about matters covered by the plan's notice of privacy practices.
- Training the employees that handle PHI.
- Implementation of appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. Note if the PHI is maintained in an electronic format, the more detailed and stringent procedures set forth in the HIPAA security rule also apply.
- Provision of a complaint procedure.
- Development and application of appropriate sanctions for employees who improperly use or disclose PHI.
- Mitigation of harmful effects cause by violations of the privacy rule.
- A prohibition against intimidation or retaliation against employees who exercise their rights under the privacy rule.
- Creation and implementation of a privacy policy.
- Maintenance of documentation required by the privacy rule.

It's worth noting that while the employer is responsible for making sure that these requirements are met, an employer can hire an independent third party to actually perform the duties. For example, compliance with the requirements regarding administrative, technical and administrative safeguards can be especially difficult and time consuming. That said, the plan remains responsible for any failure to meet the regulatory requirements.

12. What is the liability for violating the privacy rule?

There are both civil and criminal penalties.

The civil penalties apply to the plan and its business associates. The actual penalty amounts will vary based on level of culpability and the existence of aggravating or mitigating circumstances, but they can be as high as $1,500,000 per calendar year for all violations of a specific requirement.

The criminal penalties apply to any person who knowingly obtains and discloses individually identifiable health information in violation of the HIPAA privacy rules. As with the civil penalties, the sanctions vary according to the nature of the act and intent of the violator, but can be as high as fines of up to $250,000 and 10 years in prison.

13. This FAQ has focused on the obligations of employers with self-insured plans. What about employers with fully-insured plans?

Employers with fully-insured health plans typically get no PHI (other than enrollment information and very high level summary reports). In general, these employers do not have to be concerned about the requirements of the privacy rule. However, if the employer does get any other PHI, then the considerations discussed in this FAQ will apply.

It's worth a reminder that even employers with fully-insured major medical plans may still have self-insured health plans in the form of an HRA or FSA.