

## **HIPAA Privacy Compliance Basics for Plan Sponsors**

You may remember the panic last year as everyone struggled to understand the lengthy and complex privacy rules under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and then scrambled to come into compliance by the April 14, 2003 deadline. Even though the second compliance deadline (April 14, 2004, applicable to most small health plans) has passed, it is still important to revisit what the privacy rules are and how they may affect you and your health plans.

### ***Who is Subject to the Privacy Rules?***

Under the privacy rules, a "covered entity" is a health plan, health care provider or healthcare clearinghouse. The definition of "covered entity" does not include plan sponsors, and so plan sponsors are not directly regulated by the privacy rules. However, plan sponsors are inevitably affected by the privacy rules nonetheless. The extent to which the plan sponsor must comply with the regulations will depend upon many factors such as the need for access to protected health information ("PHI"), what kind of health plans are sponsored, and how they are administered.

There is a limited exception for some small health plans. Those health plans with less than 50 participants that are self-administered and self-funded are not subject to the HIPAA privacy rules.

### ***Plan Sponsors of Fully-Insured Plans***

Plan sponsors with fully-insured plans may only be affected by the privacy rules to the extent that they will be limited in their access to the PHI of plan participants due to the restraints on disclosure that the privacy rules place on the health plan insurers and health care providers. Practically speaking this may mean changing internal administrative processes to limit the PHI needed by the plan sponsor and/or getting employee authorizations before any disclosure can be made by the insurer or provider. Plan sponsors who want to continue to have regular and significant access to PHI may need to voluntarily subject themselves to the privacy rules by amending their plans and certifying compliance with the privacy rules to the health plan (insurer). Also, plan sponsors of fully-insured plans may still be subject to the privacy rules if they sponsor a health flexible spending account (called a "health FSA"). Note that health information received through the plan sponsor's role

as employer (“employment records”) is not considered PHI. There are other exclusions from PHI such as summary health information and information used and disclosed for purposes of workers’ compensation administration.

***Plan Sponsors of Health FSAs and Other Self-Insured Health Plans***

It may come as a surprise to many that health FSAs are “health plans” subject to the privacy rules. A “group health plan” is defined under the Employee Retirement Income Security Act of 1974 (which you may know as “ERISA”) as an employee welfare benefit plan to the extent that the plan provides medical care. Accordingly, a health FSA would be a group health plan and a covered entity for purposes of the privacy rules. As a covered entity, the health FSA would have to comply with the privacy rule requirements summarized below (unless it meets the criteria described above for the exclusion of small, self-administered plans).

Plan sponsors of self-insured plans are subject to the privacy rules. While plan sponsors are not themselves “covered entities,” their self-insured plans are covered entities, and as fiduciaries of those plans, the plan sponsors, for all intents and purposes, represent the plans.

Note that while some of the administrative responsibilities under the privacy rules may be contractually shifted to business associates and limited by restricted access to PHI, the plan sponsor would most likely retain fiduciary responsibility for compliance.

***Requirements for Compliance with the Privacy Rules***

Each covered entity must analyze the uses and disclosures of PHI that occur within its operation. One of the basic requirements of the privacy rules is to limit the amount of PHI that is being used and disclosed, limit the number of people with access to PHI, and generally make sure that only the minimum necessary use and disclosure is occurring.

The privacy rules have many administrative requirements and a covered entity must ensure compliance with those requirements, among others. For example:

- Establish privacy procedures, including procedures for:
  - safeguarding PHI;
  - receiving and responding to complaints; and

- providing sanctions for violations.
- Provide employees with the right to review, amend and receive an accounting of all of their PHI;
- Appoint a privacy official;
- Train employees regarding the appropriate use and disclosure of PHI;
- Distribute and maintain a privacy notice; and
- Enter into contracts with business associates regarding compliance with the privacy rules.

*For Further Information and Assistance*

There are many helpful resources available to help you understand your obligations under the privacy rules.

You may wish to access the following helpful websites for more official information on the privacy rules:

Centers for Medicare & Medicaid Services:

<http://www.cms.hhs.gov/hipaa/>

U.S. Department of Health & Human Services, Office for Civil

Rights: <http://www.hhs.gov/ocr/hipaa/>

Also, if you would like information and advice regarding the privacy rules and their application to your particular situation, or if you have other benefits questions, please contact Kathleen Bass at (949) 660-0486 or Alison Fay at (949) 660-0482.