



## ARE YOU READY TO COMPLY WITH HIPAA'S PRIVACY RULES?

Effective April 14, 2003, the privacy rules under the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA") will take effect. The good news for most employers is that they are not generally considered "covered entities" under HIPAA and, thus, not directly subject to HIPAA's complete regulations.

However, many companies will be required to comply with various aspects of the privacy rules based on their relationship to their group health plans. The law requires employers who receive employee "protected health information" ("PHI") in order to perform certain plan functions to adopt special procedures for handling PHI.

This newsletter summarizes key information employers need to know about complying with HIPAA, including a checklist of to-do items.

### Overview

The HIPAA privacy rules generally prohibit use or disclosure of an employee's PHI for any purpose, except as authorized by the employee, or as explicitly required or permitted by the privacy rules. PHI is defined to include all medical records or other individually identifiable health information in any form, whether written, oral or electronic.

The privacy rules generally apply to all types of employee group health plans. An exception applies for group plans that (a) have fewer than 50 participants, and (b) are also administered by the same employer that established and maintains the plan. Thus, as of April 14, many group health plans will not be permitted to disclose PHI to the employer or plan sponsor, or anyone else, except pursuant to the technical requirements of HIPAA's privacy rules. (Small plans with annual receipts under \$5 million have an extra year before they need to comply.)

To understand how HIPAA may affect your dealings with your employee health plan, you must analyze your current use, if any, of PHI, and decide whether you intend to continue to receive PHI for plan administration purposes. If your company will be receiving PHI, then you will need to implement certain procedures to protect the privacy of that information.

### Obligations of Employers

An employer's obligations vary depending upon several factors, including whether its group health plan is third-party-insured vs. self-insured, the type of information the employer receives from the plan, and the purposes for which that information is obtained. Here are three examples.

*Example 1:* The employer receives only "summary health information" (i.e., statistical data with no individually identifiable information) from a fully insured, third-party group health plan, and the employer uses this information only for limited purposes, such as "shopping the plan." Since the plan does not disclose any PHI to the employer (and assuming the employer does not separately create, maintain or receive PHI), the employer is not subject to HIPAA's privacy rules. Instead, the plan's third-party insurer is the covered entity obligated to comply.

*Example 2:* The employer sponsors a group health plan and receives PHI from the plan to enable the employer to perform limited, plan-related administrative functions, such as quality assurance, claims processing, and audits. In this case, the employer/sponsor must agree to comply with the HIPAA privacy rules as a condition of gaining access to the PHI, and the employer must adopt appropriate procedures for handling PHI by the compliance deadline date.

*Example 3:* The employer self-insures a group health plan, with full access to members' PHI. The employer in this case is subject to all the HIPAA requirements since it is a covered entity when functioning as the group health plan. While a contractual arrangement with a third party to administer the plan (e.g., an HMO or an insurance company acting only as plan administrator), may shift many of the requirements to the third-party administrator, the employer nevertheless retains several HIPAA compliance duties, such as issuing a notice of privacy practices to its members/employees, amending plan documents, and appointing a privacy officer to develop and implement internal privacy policies.

cont...

---

Given the broad scope of the HIPAA privacy rules, no single solution will work for every employer. Rather, each employer must analyze the structure and operation of any group health plan it offers (including vision and dental plans and flexible-spending accounts) to determine the appropriate course of action.

### ***Compliance Checklist***

1. Employers like those in *Example 2* above, who receive PHI to perform only plan administration functions, must comply with the following requirements when the HIPAA privacy rules take effect:

- *Amend Health Plan Documents* - Among other things, plan documents must provide that: (a) members will have access to their own PHI plus the ability to request amendments to and disclosures of that PHI, and (b) the plan sponsor's use and disclosure of PHI will be limited to the purposes allowed in the privacy rules, which exclude, for example, using such information for employment-related functions.
- *Erect Firewalls* – Procedures must be implemented to limit access to, and dissemination of, PHI on a strict need-to-know basis, and even then only in the minimum amount necessary for each authorized recipient to perform his/her plan-administration duties, all in accordance with the HIPAA privacy rules.

**Practice Tip:** Any employer that currently receives PHI solely to perform limited plan administration functions would do well to consider whether it wants to continue this practice. An employer could delegate the administrative functions to a third party or only receive “summary health information” to help avoid HIPAA compliance burdens.

2. Employers who sponsor self-insured, group health plans face further compliance requirements, including:

- *Business Associate Agreements* – Contracts with third-party administrators of group health plans or other entities that receive PHI (“business associate agreements”) must provide for compliance with the HIPAA privacy rules.
- *Other Administrative Requirements*
  - Notify plan members of privacy policies.
  - Appoint a privacy official to oversee compliance.
  - Implement further data-security procedures to protect PHI.
  - Establish an internal complaint process.

If you would like advice or assistance in meeting the HIPAA compliance requirements, or for additional information, please contact **Stephen M. Cowherd** or **Patricia D. Weitzman** of our office at 203-222-0885.

\*\*\*