"Your Offsite HR Department"

12062 Valley View Street, Suite 215 • Garden Grove, CA 92845
Voice 714.799.1115 • Fax 714.898.2731
website: www.hr-network.net

HIPAA Privacy Requirements

As of April 14, 2003, many organizations must begin complying with the Health Insurance Portability and Accountability Act (HIPAA) privacy regulations (April 14, 2004 for smaller health plans with less than $5 million in annual receipts). These regulations are intended to protect consumer health information.

The regulation requires "covered entities" to ensure that "protected health information" is not misused or improperly disclosed. In addition, covered entities must establish clear procedures to protect patient privacy.

For companies that provide group health care benefits, you will have some compliance obligations, particularly if you provide a self-insured health plan.

Basic Administrative Obligations for Covered Entities
As a general rule, covered entities (insurers, providers, clearinghouses, and health plans) cannot use or disclose PHI without the consent or authorization of the person the information pertains to, except as permitted or required by law.

To meet this obligation, covered entities must comply with a number of administrative requirements. For example, they must provide privacy notices to affected individuals, designate a privacy official for the organization, and establish privacy policies and procedures concerning protected health information. In addition, they must establish appropriate administrative, technical, and physical safeguards to prevent improper disclosure of health information.

Most group health plans also must amend their plan documents to restrict uses and disclosures of Protected Health Information (PHI) by plan sponsors. The rule also imposes additional specific obligations on health care providers, health plan clearinghouses, and group plan providers regarding when and how they can use PHI.

Employer Obligations if Not a Covered Entity
If your company is not specifically a covered entity, you may still need to comply with the HIPAA privacy rule regarding the flow and use of protected health information, as a result of your role as a health plan sponsor. The extent of your obligations depends on the functions you perform on behalf of the health plan.

Below are the different levels of obligation you have an employer, depending on the

type of plan you offer, beginning with the least amount of compliance required.

1. **Fully insured plans** that receive only summary health information and do not perform plan administration functions.

> A group health plan has limited obligations under the privacy rule, if it:
>
> (1) provides benefits "solely" through an insurance contract with an insurer or HMO; and (2) does not create or receive PHI, except for "summary health information" or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from an insurer or HMO.
>
> If your plan meets the above criteria, you only have to comply with two administrative requirements:
>
> (1) adopt an anti-retaliation policy stating that you will not retaliate against any individuals who exercise their rights under the privacy rule; and
>
> (2) adopt a policy stating you will not require individuals to waive their rights under the rule. You do not have to amend your plan documents or provide a privacy notice.

2. **Self-insured group health plans** that receive only summary health information and that do not perform plan administrative functions.

> A self-insured plan creates more obligations for employers, even if you receive only summary health information. In this case, you still must comply with all of the administrative requirements of covered entities (described above). The privacy notice for larger employers should be distributed to all employees enrolled in the health plan on or before April 14, 2003, and, for smaller health plans, on or before April 14, 2004. Any employees who enroll after these dates should receive the notice upon enrollment.

3. **Self-insured group health plans** that perform plan administration functions.

> Employers that provide these plans must comply with the same obligations as self-insured plans that receive only summary health information. In addition, you must amend the health plan documents to permit the disclosure of PHI from the plan to the employer for plan administration purposes. Further, you must certify to the plan that the PHI will be used only as permitted by the privacy rule. Duties under the certificate include preventing the unauthorized use or disclosure of PHI and providing "firewalls" to limit access to PHI except by specifically identified employees.

4. **Fully insured plans** that perform plan administration functions.

Employers with these plans must amend the plan documents, implement the administrative requirements, and provide the above certification to the insurer or HMO since PHI will be received. Regarding the notice requirements, these plans only have to provide the privacy notice to a plan participant upon request. The insurer or HMO is responsible for providing a separate privacy notice to participants.

Glossary of Terms

“Covered entities" are defined as health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions electronically (such as electronic billing and funds transfer).

A health plan is further defined to include a group plan that provides, or pays the cost of, medical care, as well as insurers and HMOs. The rule, however, specifically excludes plans that have less than 50 participants and are self-administered. Most employers that offer welfare benefits to employees under the Employee Retirement Income Security Act
(ERISA), whether insured or self-insured, will effectively be covered by the regulation in their role as plan sponsor.

"Protected health information" (PHI) includes all medical records and other individually identifiable health information held or disclosed by a covered entity in any form, whether communicated electronically, on paper, or orally. For example, information relating to a previous health condition, illness, propensity for a disease, and health care treatment is considered PHI, as is information relating to the payment for health care services received.

Note: **"Employment records"** held by an entity in its role as employer are not covered. The rule does not specifically explain what employment records are exempted. However, these records include any medical information needed by an employer to carry out its obligations under the Family and Medical Leave Act (FMLA), the Americans with Disabilities Act (ADA), and similar laws. In addition, the exemption includes files and records related to occupational injury, disability insurance eligibility, sick leave requests, drug screening results, and fitness-for-duty certifications. (Of course, you still must comply with the FMLA and ADA provisions that require keeping medical records confidential.)

"Plan administration functions" include claims procedures and benefit determinations.

"Plan sponsor functions" are more limited and include enrollment and disenrollment activities.

"Summary health information" consists of claims history, expenses, or types of claims stripped of certain personal identifiers. Under this definition, an employer may receive summary health information if it agrees to limit its use of the information to obtaining bids for providing health insurance coverage to group health plans or to modifying, amending, or terminating the group health plan. If the summary identifies participant information, the plan must inform individuals of the disclosure.