

Protecting the Privacy of Employee Medical Information— Six Steps Toward Compliance

Last month we presented for our clients a series of HR Network Breakfast Briefings on protecting employee medical information. This Alert is intended to assist our clients in complying with the so-called “Privacy Rule” under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).

In 1996 President Clinton signed HIPAA into law. The immediate impact of HIPAA was to require health plans to issue certificates of creditable coverage to help plan participants transfer to new health plans without the imposition of pre-existing condition exclusions and limitations. Waiting in the wings in 1996 was a directive to Congress to enact legislation that would protect patients’ medical privacy, or if Congress failed to enact such legislation, a directive to the Department of Health and Human Services (“HHS”) to adopt rules accomplishing the same result. Since Congress failed to enact medical privacy legislation, HHS, in November of 1999, issued proposed medical privacy rules as required by HIPAA. HHS received nearly 60,000 comments on these proposed rules, a number indicating keen interest in their requirements. HHS issued final rules in December 2000, proposed amendments to the final rules in March 2002, and in August 2002, the revised final rules (the “Privacy Rule”). The Privacy Rule will become effective on April 14, 2003 for all covered entities other than small health plans. Small health plans have an extended effective date of April 14, 2004. Small health plans are insured plans with total annual premiums of less than \$5 million and self-insured plans with total annual claims of less than \$5 million.

General Rule and Definitions

The Privacy Rule provides that a Covered Entity (defined below) may not use or disclose Protected Health Information (“PHI” defined below), except (i) for treatment, payment and plan operations, (ii) with the authorization of the individual who is the subject of PHI, or (iii) as permitted or required by the Privacy Rule. When using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must take reasonable steps to limit PHI to the minimum information necessary to accomplish the intended purpose of the use, disclosure or request.

Covered Entities are defined as health care providers, health care clearinghouses and health plans. Health plans include insured and self-insured group health plans and HMOs, flexible benefit plans with medical savings accounts, employee assistance plans and wellness benefit programs. Employers and other sponsors of health plans are not Covered Entities.

Health Information is defined as any information that is created or received by a Covered Entity or an employer and relates to the past, present or future physical or mental health of an individual. Individually Identifiable Health Information is Health Information that is created or received by a Covered Entity or an employer and identifies the individual (including by name, address or social security number) who is the subject of the Health Information or with respect to which there is a reasonable basis to believe

the information can be used to identify the individual.

Protected Health Information (PHI) is Individually Identifiable Health Information that is transmitted or maintained by or in electronic media or is transmitted or maintained by or in any other form or medium. For example, PHI may be contained in paper documents and files, magnetic tapes, CDs, Internet transmissions and oral discussions.

Special Provision for Employers

A special provision of the Privacy Rule permits a health plan, health insurance carrier or HMO to disclose PHI to the employer, as plan sponsor, if certain conditions are met. First, the health plan documents must be amended to:

- Describe how the employer will use PHI;
- Identify employees who will have access to PHI and under what circumstances;
- Establish a method for resolving any issues of non-compliance; and
- Provide that the health plan will disclose PHI to the employer only if the employer provides a certification of its agreement to certain conditions designed to safeguard PHI.

The employer’s certification must set forth its agreement:

- Not to use or disclose PHI other than as permitted or required by the health plan or by law;
- To ensure that its agents similarly will safeguard PHI;
- Not to use or disclose PHI for employment-related actions;

- To report to the health plan any impermissible use or disclosure;
- To provide plan participants with the ability to review their PHI and to amend or correct their PHI;
- To maintain records sufficient to provide plan participants with an accounting of the uses and disclosures of their PHI;
- To make its policies and procedures, books and records relating to the use and disclosure of PHI available to HHS for audit purposes;
- If feasible, to return or destroy all PHI received from the health plan once such PHI is no longer needed; and
- To ensure that adequate separation exists between the health plan and the employer to protect the confidentiality of PHI.

Enforcement and Penalties

The Office of Civil Rights of HHS (which will enforce the Privacy Rule) has publicly announced that it will respond to complaints of violations of the Privacy Rule by working with the Covered Entity that is the subject of the complaint to bring that entity into compliance. In addition, civil and criminal penalties, including imprisonment, may be imposed on Covered Entities for certain violations of the Privacy Rule. However, because employers are not Covered Entities, they are not subject to these penalties.

Compliance Steps for Employers

1. Assess how the Privacy Rule Affects Your Company

Employers are not Covered Entities; however, as sponsors of group health plans (particularly self-insured group health plans), employers may be responsible for some of the compliance steps described below since group health plans are Covered Entities. As stated above, group health plans include flexible benefit plans and employee assistance plans, which usually are self-insured plans that may potentially require the employer to take on more responsibility for complying with the Privacy Rule than would be the case with fully insured group health plans.

Business Associates are persons or entities that perform certain functions or activities

that involve the use or disclosure of PHI on behalf of, or provide services to, a Covered Entity. Employees are not Business Associates of their employer. Business Associates include third party administrators, COBRA compliance administrators, and attorneys whose legal services to a health plan involve access to PHI. Covered Entities are required to enter into business associate contracts with their Business Associates. Business associate contracts must:

- Describe the permitted and required uses of PHI by the Business Associate;
- Provide that the Business Associate will not use or further disclose PHI other than as permitted or required by the contract or as required by law; and
- Require the Business Associate to use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by the contract.

2. Examine Your Company's Service Provider Relationships

Sponsors of group health plans should identify the Business Associates that provide services to their group health plans, including any flexible benefit plan, employee assistance plan, and wellness benefit program. Health plans should enter into a business associate contract with each of its Business Associates. Business associate contracts should be executed by April 14, 2003 (or April 14, 2004 for small plans). An extended deadline of October 14, 2003 is available for large plans where the service contract between the Covered Entity and the Business Associate is already in place and would not otherwise come up for renewal before April 14, 2003.

3. Make Required Plan Document Amendments and Certifications

As described above, health plan documents must be amended in order for the employer to receive PHI from the health plan, and the employer must certify to the health plan its commitment to safeguard PHI. To back up that certification, employers should create a so-called firewall between the group health plan and the human resources department and ensure that PHI is not used or disclosed

for employment purposes or for the purposes of a benefit plan other than the health plan. Note that medical information needed for an employer to carry out its obligations under the FMLA, ADA, and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave, drug screening, workplace medical surveillance, and fitness-for-duty tests of employees may be part of the employment records maintained by an employer and are not PHI.

4. Employee Communications

Employers sponsoring self-insured plans (including flexible benefit plans and employee assistance plans) must prepare and distribute a Notice of Privacy Practices. Electronic distribution of this notice is permitted. Employers sponsoring insured group health plans may rely on the insurance company to distribute the Notice of Privacy Practices for the health plan, but the employer should be aware that employees will be receiving such a notice from the insurance company and be prepared to answer questions regarding it. Some sponsors of self-insured plans may rely on the third party administrator to prepare and distribute the Notice of Privacy Practices, particularly if the administrator is an insurance company; however, the business associate contract between the health plan and the administrator should specifically cite preparation and distribution of the notice as one of the administrator's duties under the contract.

5. Employee Training

Identify the employees who should be trained in the permitted uses and disclosures of PHI under the Privacy Rule. Companies should train their benefits staff and possibly the HR staff as a whole, as well as managers and supervisors. Train the benefits staff first and implement firewalls to protect PHI. Train HR staff next and implement the prohibition against improper use of PHI. Finally, train managers and supervisors regarding the impact of the Privacy Rule on the use and disclosure of PHI for purposes

other than treatment, payment and plan operations. Track and document all training.

6. Prepare for Impact of Privacy Rule on Employees

The Privacy Rule will affect employees' relationships with employer-sponsored call centers and the HR department. Employees may be required to contact only designated persons with regard to their issues and concerns related to health plans. Employers will have to communicate these changes to their employees and should be prepared to respond to grievances with the new systems.

Under the Privacy Rule, employees must have access to their PHI. They may review it, amend it and receive an accounting of its use and disclosure. Accordingly, employers must have policies and procedures in place that will allow employees to gain access to their PHI and receive an accounting of its use and disclosure. ■

Key Attorney Contacts

Amy Hartman	720/566-4110 a2hartman@cooley.com
Thomas Reicher	415/693-2381 treicher@cooley.com
Thomas Welk	858/550-6016 twelk@cooley.com
Alison Wright	415/693-2286 awright@cooley.com

This information is a general description of the law and is not intended to provide specific legal advice.

Copyright © 2003 Cooley Godward LLP. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley Godward LLP as the author. All other rights reserved.