Report on
PATIENT PRIVACY
Volume 4, Number 4 • April 2004

Employers & HIPAA: Understanding 'Group Health Plans'

This article and the Glossary on p. 3 were written by Brian D. Gradle of Hogan & Hartson, LLP, Washington, D.C. For more information, contact Mr. Gradle at BDGRADLE@HHLAW.COM.

While HIPAA privacy compliance has focused on the health care industry — including physicians, hospitals, insurance and managed care companies, and clearinghouses — the implications of the privacy rule to businesses *outside* of the health care industry, as well as to health care companies *in their capacities as sponsors of group health plans* — remain overshadowed, misunderstood, or ignored.

But the privacy rule cuts an enormous swath through all sectors of American business. Indeed, it creates federally mandated requirements regarding protected health information (PHI) that can impact any business, regardless of its size, location or industry.

Any Employer Could Have a Covered Plan

The privacy rule's definition and regulation of "health plans" includes not only insurance companies and managed care organizations, but also employer-sponsored "group health plans," whether they are (a) "fully insured" by HMOs, PPOs, or other insurers, or (b) "self-insured" by the employer bearing the costs associated with such plans (see "Glossary").

On April 14, 2004, all group health plans — except for very small, self-administered ones that are exempted from compliance — are subject to privacy rule compliance, if they weren't already. While April 14, 2003, was the compliance deadline for most HIPAA covered entities (including large group health plans), group health plans were given an additional year to comply if they had less than $5 million in premiums (if fully insured) or claims (if self-insured).

Because group health plans usually do not have a separate corporate existence — they frequently are comprised by the plan documents, such as summary plan descriptions, that describe the plan's benefits and obligations — it generally falls to the plan sponsor or to a third party retained by the plan sponsor (e.g., a TPA) to administer and operate the group health plan. Consequently, employers that are plan sponsors confront two fundamental HIPAA compliance issues:

(1) Ensure that the group health plan complies with its obligations under the privacy rule; and

(2) Ensure that it — as plan sponsor — complies with the privacy rule regarding all PHI that it receives. On this issue, it is particularly important that the firewall requirement (see "Glossary") is satisfied, in order to ensure that PHI is not used for employment-related purposes.

In light of these indirect obligations, it is essential that employers — regardless of the nature of their business — conduct a HIPAA privacy assessment and evaluate the HIPAA compliance obligations they may face. One way to commence this assessment is to answer the following questions regarding each of their group health plans:

(1) Is the group health plan fully insured or *self-insured*?

(2) What health information is provided to the *employer* — either directly, or in its capacity as an administrator of the group health plan — regarding the plan's participants?

Five Scenarios and Their Implications

Five different scenarios are depicted below to help understand the repercussions of these two questions. They describe the varying privacy rule obligations that will be imposed upon a company's group health plan, depending upon the type of plan it is, and the nature of the health information provided to the employer.

Scenario 1: A small car dealership in the Midwest sponsors a group health plan for its employees that it self-administers. There are 37 "participants" in the plan, which includes both current and retired employees.

Privacy Rule Implications: None.

Comment: Employee welfare benefit plans that are self-administered *and* have fewer than 50 participants are not considered "group health plans" for purposes of the privacy rule. The car dealer's plan satisfies these criteria and consequently is not a "group health plan" for purposes of the privacy rule and is not subject to its requirements. Of course, the employer would remain subject to applicable state laws regarding employee privacy, notwithstanding the exclusion of its health plan from the privacy rule.

Scenario 2: A boat maker in the Pacific Northwest administers its large, self-insured group health plan. Its claims annually are in excess of $5 million.

Privacy Rule Implications: Significant.

Comment: For starters, as a "large" health plan, the privacy rule compliance date was April 14, *2003*. Then,

because the plan is self-administered, there is a tremendous amount of health information handled by the plan that must be appropriately protected. Under the privacy rule, the boat maker's *self-insured health plan* is the covered entity subject to HIPAA, and therefore the plan must comply with the privacy rule's administrative requirements, including:

◆ Appoint a Privacy Officer.

◆ Appoint an individual or office to handle privacy complaints from health plan participants.

◆ Disseminate a Notice of Privacy Practices to plan participants.

◆ Identify and train members of the company's workforce who will access PHI to administer the plan, and implement administrative, physical, and technical safeguards to protect the PHI.

◆ Enter into business associate agreements with vendors, contractors, and other third parties as required.

Develop and implement HIPAA policies and procedures, including those regarding participants' access to and amendment of health information, accounting for PHI disclosures, and imposing sanctions for privacy rule violations.

Implement policies that prohibit any workforce member from engaging in intimidating or retaliatory acts against any person for exercising his or her rights under the privacy rule, and that prohibit requiring individuals to waive their rights under the privacy rule.

As a practical matter, it will in most cases be the employer, on behalf of its group health plan, that will ensure that these administrative requirements are met. Also, before any PHI may be disclosed by the group health plan to the employer's plan administrators, the employer must amend its plan documents to:

(1) Describe the permitted uses and disclosures of the PHI;

(2) Provide that disclosure is permitted only after the group health plan receives certification from the plan sponsor that the plan documents have been amended to reflect the privacy rule's requirements (e.g., no use of PHI for employment-related decisions); and

(3) Comply with the "firewall requirement."

Certification from the plan sponsor is *not required* in order for the plan sponsor to request and obtain from the group health plan the summary health information and the enrollment/disenrollment information that is described in Scenario 4 below.

Scenario 3: At the same boat maker described in Scenario 2, the Workers' Compensation (WC) Department needs certain medical information to process a claim regarding an injured employee. The administrator of the group health plan has this information. The WC department manager approaches the group health plan's administrator, and requests a copy. Applicable state law — in this scenario — authorizes health plans to make such disclosures to employer WC administrators.

Privacy Rule Implications: Significant.

Comment: Disclosures of PHI by the plan administrator are subject to the privacy rule's restrictions. Because the privacy rule permits disclosures of PHI by covered entities as authorized by applicable workers' compensation law, the plan administrator can honor the WC administrator's request in this case, without the individual's authorization. However, in other cases — such as requests from the employer for information relevant to the employer's administration of an American with Disabilities Act (ADA) claim or a Family and Medical Leave Act (FMLA) claim — the plan administrator will need to obtain the authorization of the individual before honoring such requests. PHI that is disclosed to an employer becomes an employment record and is no longer subject to the HIPAA privacy rule.

Scenario 4: A community hospital located in the Rocky Mountains has only fully insured group health plans, and receives no health information from its insurers *other than* (1) information about employees who have enrolled or disenrolled from coverage, and (2) "summary health information."

Privacy Rule Implications: Very limited.

Comment: Fully insured plan sponsors and their group health plans are "exempt" from most of the privacy rule requirements, if the plan sponsor's plan administration functions are limited to: (1) conducting enrollment and disenrollment for the plan (such functions are considered outside of "plan administration," and health plans may disclose information to a plan sponsor regarding an individual's enrollment status) and (2) utilizing "summary health information" to obtain premium bids or to modify, amend, or terminate a group health plan. In cases such as this scenario, it is the insurance company that bears the responsibility — as the covered entity — for complying with the privacy rule on behalf of the group health plan, including providing the employees with their notice of privacy practices, entering into business associate contracts, and ensuring that only permissible uses and disclosures occur of the information occur. Consequently, the hospital's only obligations are to (1) refrain from requiring any employee to waive rights under the privacy rule as a condition to receiving plan benefits; and (2) refrain from any retaliatory or intimidating acts if any person seeks to exercise any rights under the privacy rule. If the hospital in this case added a *self-insured* health benefit to the group health plan, the group health plan

would no longer qualify for the privacy rule exemption for *fully insured* group health plans. These obligations apply to the hospital in its capacity as a plan sponsor of a fully insured group health plan, which are separate and distinct from its broader obligations under the privacy rule as a health care provider.

Scenario 5: A medical clinic in New England has a "small" group health plan, with a HIPAA compliance deadline of April 14, 2004. It is a self-insured plan that is administered by a TPA. However, the TPA regularly provides the clinic with reports containing substantial amounts of PHI — including the health claims filed by its employees and health care services provided to them.

Privacy Rule Implications: Significant.

Comment: The use of a TPA by the self-insured clinic *does not* insulate its group health plan from its status as a

Glossary of Group Health Plan Terms

Employment Records are those records that an employer maintains in its role as an employer. Although "employment records" are not defined under the privacy rule, they are expressly excluded under the rule from the definition of "protected health information." HHS has commented that medical information that is 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 to files and records relating to such things as occupational injury, disability insurance eligibility, sick-leave requests, drug screening results, workplace medical surveillance, and fitness-for-duty tests for employees, may all be part of the "employment records" that are maintained by a covered entity in its role as an employer. However, any use or disclosure of PHI — including disclosure of information that will be considered an "employment record" once it is maintained by an employer —is subject to the privacy rule.

The Firewall Requirement demands an "adequate separation" between the group health plan and the plan sponsor, including identifying employees who will have access to PHI, and restricting their use of such PHI to plan administration functions. Disclosure of PHI by the group health plan to the plan sponsor for employment-related or other administrative purposes generally requires the written authorization of the individual to whom the PHI relates, unless the disclosure is otherwise permitted under the privacy rule (e.g., is a disclosure required by law).

Health Plan means an individual or group plan that provides or pays for the cost of medical care. It includes group health plans, but excludes certain "excepted benefits," including accident or disability income insurance, liability insurance, workers' compensation, and coverage for on-site medical clinics.

Group Health Plans are employee welfare benefit plans, including fully insured and self-insured plans, that provide medical care to employees and dependents through insurance, reimbursement, or otherwise, and that (i) have 50 or more participants, or (ii) are administered by an entity other than the employer that established and maintains the plan.

Participant means any employee or former employee, or any member or former member of an employee organization, who is or may become eligible to receive a benefit of any type from an employee benefit plan that covers employees of such employer or members of such organization, or whose beneficiaries may be eligible to receive any such benefit.

Plan Sponsor means the employer or the employee organization, or both, that establishes and maintains an employee benefit plan. Plan sponsors of group health plans are not themselves, however, HIPAA covered entities.

Self-Insured Plans are plans under which a sponsoring individual or organization (such as an employer) assumes the financial risk for paying the health care that is provided under the plan. Self-insured plans include flexible spending accounts (FSAs) that permit employees to pay for uninsured medical expenses on a pre-tax basis.

Summary Health Information is information that summarizes the claims history, claims expenses, or type of claims experienced by individuals under a group health plan. Summary health information contains no individually identifiable information, *except that* it may contain geographic information that is aggregated to the level of a 5-digit zip code.

Third-Party Administrator is an entity that provides certain services such as billing, claims processing, utilization review, quality assurance, network development and management, and plan document development. Third party administrators are *business associates* to the health plans for which they provide such services.

HIPAA covered entity. Consequently, while a business associate agreement with the TPA is essential — and will set out the HIPAA functions and the responsibilities that the TPA will provide — the group health plan will remain a covered entity subject to the privacy rule and its requirements. Of concern in this scenario is the significant amount of PHI that is being provided to the clinic. If the clinic has retained responsibilities for plan administration (e.g., handling appeals of benefit claims that are denied by the TPA), then the clinic can obtain PHI from the TPA for such purposes as long as the clinic — as plan sponsor — has amended its plan documents, identified its employees that will provide the plan administration services, and otherwise complied with the requirements described in Scenario 2 above. If the clinic *has not* retained such plan administration responsibilities, or if such plan amendments, employee designations, and other administrative steps have not been taken, then the PHI disclosures should be limited to the summary health information and enrollment/disenrollment information described in Scenario 4. ✧