SMALL BUSINESS PLANS

What Small Employers Need to Know About HIPAA

Although employers are not directly regulated under HIPAA, those offering health benefits are ultimately responsible for the compliance of the group health plans they sponsor. Now that the first effective date has passed and the second date is rapidly approaching, this is a good time to ask what is in store for smaller health plans based on the experience of their larger counterparts.

BY FREDRIC S. SINGERMAN AND PAUL S. HORN

Fred Singerman is a partner in the law firm of Seyfarth Shaw specializing in pension, employee benefits, and executive compensation matters. His e-mail address is fsingerman@dc.seyfarth.com or view the firm's Web site at www.seyfarth.com.

Paul Horn is the benefits director at American Systems Corporation. His e-mail address is paul.horn@2asc.com.

The extensive privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) became effective for health care providers and larger health plans on April 14, 2003. For these covered entities, this past April 14 marked the conclusion of an exhaustive investigation of all business practices and relationships involving the use or transmission of protected health care information. HIPAA becomes effective for "smaller" health plans on April 14, 2004.

Who Will Be Covered on April 14, 2004?

"Covered entities" under HIPAA include (a) health care providers (e.g., doctors, hospitals, and pharmacies) that transmit certain types of patient information electronically, and (b) health plans (e.g., health maintenance organizations [HMOs] and health insurers). Covered health plans also include employer-sponsored medical, dental, mental health, and prescription drug and vision plans, as well as employee assistance plans (EAPs) that provide ERISA-covered health benefits and health flexible spending accounts (FSAs). Disability, workers' compensation, and life insurance plans are not covered, even though smaller employers may receive more sensitive health information from these plans than from their insured health plans.

The April 14, 2003, effective date applied to all covered health care providers and to health plans with annual receipts in excess of $5 million. A "small" health plan—one having annual receipts of $5 million or less—has until April 14, 2004, to comply. In determining annual receipts, a fully insured health plan should use the amount of total premiums paid for health insurance benefits during the plan's last full fiscal year. Employee-paid premiums are included for this purpose. Self-insured plans, both funded and unfunded, should use the total amount paid for health care claims by the employer or benefit fund. However, premiums for stop-loss insurance paid by an employer sponsoring a self-insured plan are not counted under guidance issued by the Department of Health and Human Services (HHS). HHS guidance does not appear to require that health plans (e.g., medical, dental, and health FSAs) that are maintained as separate legal entities be aggregated in determining whether the plans meet the $5 million threshold.

Are Any Plans Exempt from HIPAA?

The HIPAA privacy rules do not apply to an employer's self-administered group health plan with fewer than 50 participants.

Perhaps more important, a health plan, regardless of size, is exempt from almost all of HIPAA's administrative requirements, if (1) the plan provides health benefits only through an insurance contract with a health insurer or an HMO, *and* (2) the plan does not create or receive any individually identifiable "protected health information" other than summary health information (deleting all identifying information other than some geographic information) and basic enrollment and disenrollment information.

While many employers with insured plans would appear to fall within the insured health plan exemption, the exemption applies only if the employer does not perform health plan administrative functions and *also* does not hire a third party to perform such func-

tions (other than an insurer or HMO). Thus, the exemption will not be available to an employer who self-administers COBRA or HIPAA certificates of coverage, or outsources these functions to an entity other than the insurer or HMO. Furthermore, since a health FSA is inherently a self-insured health plan, any employer who maintains a health FSA with at least 50 participants will need to comply with the HIPAA requirements discussed below, even if its other health plan arrangements are fully insured.

An obvious question is why must an employer comply with HIPAA's extensive documentation requirements when it outsources most, if not all, of its health plan functions and never has access to sensitive health information. For a self-insured plan, the reason is that the regulations apply to the health plan as an entity, and the employer will normally be the plan administrator. Thus, when employers outsource their health plan administrative functions to third-party administrators (TPAs) and other administrative service providers, called "business associates" under HIPAA, the employer must enter into an agreement with the business associate requiring HIPAA compliance. This is how these outsourcing arrangements are brought within HIPAA's privacy requirements.

It is less clear why employers with insured health plans should be required to comply with HIPAA's documentation requirements merely because they process COBRA elections and premium payments. The problem may stem from the broad definition of "protected health information" (PHI) as any information in electronic, paper, or oral form that is created or received by a health care provider, health plan, or employer that relates to "the past, present, or future physical or mental health or condition of an individual … or the past, present, or future payment for the provision of health care" and that identifies or could be used to identify an individual. HHS interprets this definition as covering information about the individual's health insurance coverage, so that COBRA election information would be covered.

HHS recognized that this broad definition of PHI could be construed to cover the entire payroll process, since employees would "reveal" PHI when they enroll for coverage and agree to have contributions withheld from their pay. To limit the unintended application of the privacy rules, HHS clarified that the employer acts in its capacity as *employer*, rather than as health plan sponsor, in doing enrollment and payroll processing. The regulations were even revised to make clear that information that an employer receives in its capacity as employer—rather than on behalf of a health plan—is not protected health information under HIPAA. This would also include, for example, information submitted in connection with a workers' compensation or disability claim or a doctor's back-to-work note. However, COBRA processing and HIPAA certificates are inherently health plan administration functions, rather than employer functions, since they normally apply when the individual has left employment.

What Does HIPAA Compliance Require?

Basically, HIPAA's privacy rules involve three main components: (1) limitations on the use and disclosure of PHI; (2) administrative requirements; and (3) individual rights of health plan participants. These requirements apply to employer health plans that are not exempt from HIPAA's privacy rules. Note that an employer sponsoring an insured health plan to which the exemption applies will still need to amend its health plan document if it intends to receive summary health information from the insurance company or HMO. In addition, the employer must refrain from (a) intimidating or retaliatory acts against individuals who exercise their privacy rights under HIPAA, or (b) requiring a waiver of HIPAA rights as a condition for participating in the plan.

1. Operational limits on the use and disclosure of PHI. A group health plan is permitted to use and disclose PHI only as necessary for "payment" or "health care operations" purposes. Thus, when employees are designated by the health plan sponsor as responsible for health plan functions, these employees will be able to perform the functions necessary for the normal operation of the plan. Since human resources and benefits professionals already make it a practice not to disclose personal employee information, most employers will see relatively few operational changes as a result of HIPAA.

"Payment" includes actions taken by a health plan to obtain premiums, determine or fulfill its responsibility for coverage or the provision of benefits, or obtain or provide reimbursement for health care. This would include, for example, getting premium payments, making eligibility determinations, and processing COBRA elections. "Health care operations" include the plan's administrative and organizational activities, such as securing contracts for health insurance or health benefits, arranging for third-party administration, legal or auditing services, cost management, and utilization review. In addition, a group

health plan may use and disclose PHI to comply with applicable federal, state, and local laws (including workers' compensation laws) and to address various public policy concerns.

For most other uses or disclosures of PHI, a health plan must first obtain the participant's written authorization following specific HIPAA guidelines. However, an important exception to this general rule permits a health plan to communicate with a participant's family member or "friend" involved in the participant's health care, provided that the participant agrees to the disclosure, or if the participant is not available, the disclosure is otherwise in the participant's best interests. This exception could apply, for example, where a participant's spouse calls the plan to confirm the participant's coverage while the participant is overseas or otherwise unavailable.

2. Documentation requirements. For most group health plan sponsors, the following documentation requirements constitute the bulk of HIPAA compliance efforts:

• *Amend plan documents.* A plan sponsor must amend its group health plan documents to provide adequate separation (a "firewall") between the group health plan and the plan sponsor and to describe which employees will have access to PHI for plan administration functions.

• *Revise "business associate" contracts.* The employer will need to amend its contracts with any third parties that provide services to the health plan involving PHI to ensure that these business associates take steps to avoid violating HIPAA privacy rules. (Note that this requirement does not apply to health insurance or HMO contracts because insurance companies and HMOs are separately regulated under HIPAA.)

• *Create and adopt a privacy policy.* The health plan (through the employer) must create and maintain a written privacy policy and other documentation designed to ensure the plan's compliance with HIPAA's privacy rules. For example, the privacy policy must document (1) the designation of a privacy officer responsible for the implementation of the policy; (2) a description of the health plan's permitted uses and disclosures of PHI; (3) the safeguards implemented to protect PHI from intentional or unintentional use or disclosure in violation of the policy; (4) protocols and criteria for ensuring compliance with the rule that only the "minimum necessary" PHI can be used for payment or health care operations purposes; (5) processes for receiving and responding to participant complaints regarding policy violations and requests to exercise individual privacy rights; and (6) the sanctions that may apply to employees who violate the policy.

• *Prepare and distribute a privacy notice.* Each participant is entitled to receive a notice describing how PHI will be used or disclosed by the health plan and the new rights that participants have regarding their PHI. Small health plans should provide the notice to existing participants by April 14, 2004, and to later participants when they first enroll. A revised notice must be provided within 60 days of a material change. If the plan sponsor of an insured health plan is required to comply with HIPAA because it retains some administrative functions (such as COBRA), participants will end up receiving two notices, since the health insurer also will be sending one (not to mention the notices from the participant's doctor, pharmacy, etc.).

• *Train employees who use or disclose PHI.* Employees who perform health plan administrative functions must be trained on the health plan's privacy policy. The plan must document and keep records of its HIPAA training.

3. Individual rights. The privacy rules create the following individual rights for group health plan participants:

• *Right to access PHI.* A participant has the right to inspect and obtain PHI that is contained in records used by the plan to make decisions about the participant; these are called the "designated record set." An employer who outsources or insures its health plan functions will have few, if any, records to make plan decisions, since it will not be making any claims determinations. It may, however, have records relating to the participant's eligibility for benefits, such as enrollment records.

• *Right to amend PHI.* A participant has the right to request the group health plan amend or correct PHI in its records that is inaccurate or incomplete.

• *Right to an accounting of disclosures.* A participant has the right to receive a list of disclosures of PHI by

the group health plan within the last six years (but not before the HIPAA effective date for the plan [2004]). Disclosures for payment or health plan operations purposes, or pursuant to a participant's authorization, are not required to be included in the accounting.

• *Right to request additional restrictions.* A participant has the right to request additional restrictions on the use or disclosure of PHI, although the plan is not required to comply with the request.

• *Right to confidential communication of PHI.* A participant has a right to request that a group health plan communicate PHI to an alternate address or by alternate means. The plan must accommodate a reasonable request if the participant states that he or she would otherwise be endangered.

• *Right to file a complaint.* Any person has a right to complain to a group health plan's privacy officer about the improper use of PHI by the health plan. The plan must investigate any complaints and, if necessary, take immediate steps to mitigate the harm from a violation and to minimize the possibility of a recurrence.

Many of these rights, such as the right to access PHI or receive an accounting, place a burden on the employer to retain records relating to PHI and HIPAA compliance, generally for at least six years from when the record was created or last effective.

Sanctions for Noncompliance

Unlike most federal employment laws, HIPAA does not provide employees or other plan participants a right to sue health plans directly for privacy violations. Instead, HIPAA is enforced by the HHS, which may impose penalties of up to $100 per violation, up to $25,000, per person per year. Criminal sanctions may also apply. Given the enormous amount of resources HIPAA monitoring would require, it is most likely that HHS will become involved in a health plan matter only in response to a participant complaint.

However, it is possible that participants could sue under state privacy laws, or state employment or consumer laws, to enforce their rights. Since HIPAA contains no preemption clause and the employer has provided (on behalf of the health plan) a HIPAA privacy notice setting out the participant's privacy rights, an employee may argue that violation of these rights is actionable under a breach of contract or reliance theory.

What Now for Smaller Health Plans?

HIPAA is designed to implement commonsense privacy protections for patient health information. Most employers already follow practices to maintain the privacy of their employees' personal information, so they should see only minor change to their plan operations. For these employers, HIPAA's most significant burdens will come from the requirement to extensively document their privacy practices.

Smaller health plans should benefit from the lessons their health plan consultants and attorneys learned in gearing up for April 14, 2003. Experienced providers will rapidly be able to determine where the employer's key decision points and compliance "hot spots" are:

- Is compliance necessary at all?
- Where does the employer receive or disclose PHI?
- Which employees should be within the health plan firewall?
- What is the most efficient way to document the plan's privacy practices and train affected employees?

Although the compliance deadline for smaller health plans is April 14, 2004, employers should address business associate contracts and plan documentation as they gear up for the 2004 open enrollment. HIPAA requires that all covered entities conduct specified electronic transactions, including enrollment and claims payments, using standardized data sets, by October 16, 2003. For most employers, the insurance company or TPA will handle these transactions, and the employer will be affected only to the extent that the insurance company or TPA changes the protocol for how it receives information from the employer. The services agreement between the employer and the administrator should require timely compliance with these requirements by the administrator in advance of the October 16 deadline.

Since insurance companies and HMOs are already required to comply with HIPAA, a "small plan" employer that wants to assist a participant with a health claim matter involving PHI will generally now need to obtain a written authorization from the participant to communicate with the insurance company or HMO.