HIPAA Privacy Compliance: It’s Time to Take It Seriously

By Russell E. Greenblatt and Jeffrey J. Bakker, Katten Muchin Zavis Rosenman
© 2004 Aspen Law & Business. All rights reserved.

The privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) have been in effect for many covered entities since April 14, 2003. For small health plans, however, those with less than $5 million in annual claims or premiums, the deadline for compliance is April 14, 2004. As sponsors of these small health plans prepare to take steps to ensure compliance with the privacy rules, they can benefit from reviewing issues that have been confronted by sponsors of large health plans. This column discusses certain aspects of the HIPAA privacy rules that are likely still to cause confusion among sponsors of small health plans, based in large part on our conversations with sponsors of (and service providers to) these health plans.

Plans Covered by the HIPAA Privacy Rules

Employers who have only just begun to attempt to get a handle on the scope of their obligations under the HIPAA privacy rules might begin by determining which of their employee benefit plans are regulated by the privacy rules.

Health plans are covered entities and are directly regulated by the HIPAA privacy rules. This includes “group health plans” which are employee welfare benefit plans as defined by the Employee Retirement Income Security Act (ERISA) and includes both insured and self-insured arrangements. Consequently, as most employers would expect, plans providing medical, dental, vision, mental health, and pharmacy benefits fall within the scope of the HIPAA privacy rules. Plans that are not subject to the privacy rules include disability, life insurance, accidental death and dismemberment insurance, and, generally, workers’ compensation plans. Stop-loss insurance constitutes insurance protection provided to the health plan or plan sponsor rather than constituting a plan providing medical care, and, consequently, is excluded from direct regulation by the privacy rules.

There are certain plans that might not intuitively seem to be employer health plans, but are treated as such under the HIPAA privacy rules. As most practitioners had anticipated, the Department of Health and Human Services (HHS) took the position that health flexible spending accounts (FSAs) are generally health plans for purposes of applying the privacy rules, even though health FSAs are generally excluded from HIPAA’s portability rules. Employers considering implementing the new health care reimbursement arrangements (HRAs) should recognize that such arrangements also will be considered to be health plans subject to the privacy rules.
Employee assistance programs (EAPs) are often a source of confusion. Generally, if the services provided by the EAP are limited to assessment and referral services only, the EAP should fall beyond the scope of the privacy rules. If, however, for example, the EAP provides mental health counseling services, it will be subject to the privacy rules. Also, keep in mind that even if the EAP is not directly regulated as a group health plan, if it receives information from (or provides information to) a group health plan, it will be dealing with protected health information (PHI). Thus, attention will need to be given to how FSAs, HRAs, and EAPs receive, process, and disseminate information.

Finally, the privacy rules provide an exception for certain small group health plans. If the group health plan has fewer than 50 participants and is self-administered, it is exempt from the HIPAA privacy rules. If the plan is administered by a third party, however, it is subject to the privacy rules regardless of its number of participants. For many small employers, this may be an important distinction. As discussed below, employers who sponsor fully-insured plans have significantly fewer obligations under the privacy rules than those who sponsor self-insured plans, but even small, fully-insured plans are regulated by HIPAA. In addition, if a small, fully-insured employer were to sponsor a health FSA in addition to the insured plan, it subjects itself to several more requirements under the privacy rules than would otherwise be the case (such as the appointment of a privacy official and distribution of a notice of privacy practices). Such an employer may wish to avail itself of this exemption if the health FSA is self-administered and below the 50 employee threshold. The ERISA definition of participant is used for purposes of counting and generally includes any employee who is or may become eligible to receive a benefit of any type under the group health plan.

What Information May Be Used Under What Circumstances?

Perhaps the most challenging aspect of the HIPAA privacy rules for employers, especially for sponsors of small health plans, is determining what kind of information may be used under what circumstances. A recent article in Benefits Law Journal discusses in detail the implications of disclosing health information to employers.1

When health information is at issue, the first question an employer should ask is: “From where is the information coming?” If the information comes directly from the individual, rather than from the health plan, and is provided to the employer in its role as an employer, the information is not PHI if, and only if, the employer maintains these records separate from health care records. For example, an employee can call in sick without the employer being unduly concerned about disclosing such information. This allows an employer to meet its legal obligations under the Family and Medical Leave Act (FMLA) and the Americans with Disabilities Act (ADA), for example. It also allows employers to obtain the results from pre-employment drug tests or post-accident fitness-for-duty examinations. If the employer uses PHI from one of its group health plans, however, rather than information directly received from the employee or its own employment records, it will be necessary to obtain an authorization from that employee.

A second concern is the level of detail of the information at issue. It is important for employers to be familiar with the definitions of “e-identified information” and “summary health information.”

“De-identified information” neither identifies the individual nor provides a reasonable basis to believe that the information can be used to identify the individual. If the information is de-identified, it does not constitute PHI and thus is not subject to the HIPAA privacy rules. Consequently, an employer may use de-identified information for any purpose without soliciting authorizations or amending the plan document to permit disclosure of PHI to the plan sponsor (as described below). The level of detail that must be removed from the data for it to be considered de-identified, however, may make it of limited use to a plan sponsor of a small health plan.

A group health plan may also disclose summary health information to a plan sponsor, even without a plan amendment permitting the disclosure. Summary health information is similar to de-identified information, but more detail is permitted concerning individual zip codes. The permitted uses of summary health information (without an amendment to the plan) are limited, however, to obtaining premium bids and modifying, amending, or terminating the plan.
If an insured plan needs PHI, rather than just summary health information, for example, to obtain a premium bid in shopping for a new insurance carrier, it may do so because such actions are within the definition of health care operations. It will need to comply, however, with the plan amendment and certification requirements described below.

A health plan may use or disclose PHI for purposes of payment, treatment, or health care operations, without an authorization from the individual who is the subject of the health information. In order for this information to be disclosed to the employer for these purposes, the employer must certify that it will comply with the HIPAA privacy rules and amend the plan document to identify the permitted and required uses and disclosures of PHI, including identifying the employees who will have access to PHI and establishing firewalls to ensure separation between health plan operations and the employer’s other operations. While some sponsors of insured health plans may be able to limit their access to only de-identified or summary health information, sponsors of self-insured plans will generally require access to PHI to ensure that claims are processed and paid appropriately. Consequently, the sponsor of a self-insured plan will need to satisfy these certification and amendment requirements so that the plan may disclose PHI for purposes of payment, treatment, and health care operations. A small employer may not appreciate the distinction between its own benefits department and the plan, but HIPAA requires the employer to provide a certification to the plan in such circumstances.

To the extent the use or disclosure extends beyond payment or health care operations, the health plan will be required to obtain an authorization from the person who is the subject of the information. (The plan is not likely to need to disclose PHI for treatment purposes.)

“Payment” activities include activities such as determination of eligibility or coverage, billing, claims management, review of health care services, and utilization review activities. “Health care operations” include activities such as conducting quality assessment and improvement activities, reviewing the qualifications and performance of health care providers, performing underwriting, premium rating, and other activities relating to the creation, renewal, or replacement of health benefits and establishing budgets. The plan may disclose PHI for these purposes, including disclosures to the plan sponsor, without obtaining an individual authorization, assuming that the amendment and certification requirements have been satisfied.

Where the use or disclosure of PHI is beyond the scope of payment, treatment or health care operations, however, it generally will be necessary to secure an authorization from the individual. One activity where this need commonly arises is claims advocacy. Although some practitioners take the position that claims advocacy falls within the scope of payment activities, it would seem to be prudent to obtain an authorization (to the extent information from the health plan is being used or disclosed) because the advocate is not acting on behalf of the plan, but rather on behalf of the individual. Another common occurrence requiring authorization is communication with family members. Disclosure of PHI to family members also is beyond the scope of payment, treatment, or health care operations. A health plan may disclose PHI which is directly relevant to the requester’s involvement in the individual’s health care when the requester is a family member, relative, or close personal friend of the individual is not available to agree or object, such as when the individual is incapacitated or in an emergency situation. In other circumstances, disclosure and PHI can be made to such persons if the plan receives oral or written permission from such individual.

Notice of Privacy Practices

Sponsors of small health plans need to prepare for compliance with the requirement that plans provide participants with a notice of privacy practices. This notice is intended to inform individuals of the uses and disclosures of PHI that a plan may make, to inform individuals of their rights, and to describe the plan’s duties with respect to that protected health information. For sponsors of small health plans, this notice must be distributed by April 14, 2004, to individuals then covered by the plan. After this date, the notice must be distributed to new enrollees at the time of enrollment and to all individuals covered by the plan within 60 days of a material revision to the notice.
Many sponsors of insured health plans might assume that this task will be performed by the insurance company. The insurance company is obligated to provide this notice, but the plan sponsor should ensure that it does not have separate notice obligations based upon the employer's particular method of operations, how it deals with PHI, and what other plans the employer maintains (such as an FSA, HRA, or EAP).

If the employer only sponsors fully insured plans and the sponsor uses only summary health information and enrollment information, the employer is not required to provide a separate notice. If the plan creates or receives PHI in addition to summary health information and enrollment/disenrollment information, however, the plan is required to maintain its own separate notice and to provide such notice upon the request of any person.

The employer will have to distribute a notice to the extent it provides self-insured benefits. In some cases, these benefits may be provided pursuant to one master welfare plan, in which case one notice will be sufficient. If, however, an employer has a self-insured medical plan and a separate self-insured dental plan, for example, separate notices would be required unless the employer treats these plans as part of an organized health care arrangement (OHCA).

An OHCA may consist of a group health plan and one or more other group health plans, each of which is maintained by the same plan sponsor. (Certain other entities may also be combined to form OHCAs, such as a group health plan and a health insurance issuer.) The advantages to setting up an OHCA are that the plans that make up the OHCA may share PHI for purposes of payment, treatment, and health care operations with each other and that the plans may undertake joint activities, such as providing one comprehensive notice of privacy practices. Where two or more plans making up an OHCA distribute a joint notice of privacy practices, the notice must state that PHI will be shared among the plans, if applicable, in addition to the other elements normally required to be in the notice.

**Insured Versus Self-Insured Plans**

Small employers are likely to sponsor insured medical plans. Sponsors of insured health plans often are either unsure of their obligations under the HIPAA privacy rules or assume that they have no such obligations. This assumption may turn out to be incorrect.

Employers who only sponsor insured health plans and do not interact with PHI (other than summary health information and enrollment or disenrollment information) are exempt from most of the privacy obligations under HIPAA. Most of the obligations will fall upon the insurance company, such as preparing and distributing a notice of privacy practices.

If the employer is going to rely on this exemption, however, it needs to ensure that all of the health benefits it provides are insured. For example, if the medical plan is insured but the dental plan is self-insured, the employer will be obligated to comply with the full set of privacy rules, including appointing a privacy official, establishing firewalls, developing policies and procedures designed to ensure compliance with the privacy rules, establishing a process for handling complaints, and implementing sanctions for privacy breaches, in addition to meeting the plan amendment and certification requirements. This is where having a health FSA could be problematic, because even if the other health plans are insured, the health FSA may cause the employer to be burdened with greater HIPAA responsibilities than otherwise intended.

**Conclusion**

Sponsors of small health plans need to (1) identify covered plans and business associates who handle PHI; (2) establish policies and procedures concerning the handling of PHI (including when such information may be disclosed to the employer); and (3) satisfy the documentation requirements, including ensuring that a notice of privacy practices is distributed and amending the plan document, if necessary. These tasks must be completed by the compliance deadline of April 14, 2004.
Also, large employers should continue to come into line where they identify shortcomings with their HIPAA compliance program. The Office of Civil Rights for HHS reported that it has received almost 2,000 complaints of privacy violations which it is addressing. In several cases it may impose civil fines, and it has referred some complaints to the Department of Justice for potential criminal enforcement where the violations are egregious. Therefore, both large and small employers should ensure that they are making at least good faith efforts towards compliance with the HIPAA privacy rules.

Notes

Russell E. Greenblatt concentrates his practice in employee benefits. Before joining Katten Muchin Zavis in 1980, Mr. Greenblatt served as an Attorney Advisor with the Employee Plans and Exempt Organizations Division of the Office of Chief Counsel to the IRS (Washington, D.C.) during which time he was the principal author of the IRS regulations on VEBAs.

Mr. Greenblatt is a frequent author and lecturer on the subject of welfare benefit plans and VEBAs, including for the American Bar Association, American Institute of Certified Public Accountants, New York University Tax Institute, University of Southern California Tax Institute, Taxes, Taxation for Lawyers, The Journal of Taxation and Benefits Law Journal. He has testified before the Ways and Means Committee and the IRS on pending benefits legislation and regulations, and serves on the Editorial Advisory Board of the Benefits Law Journal, for which he authors the quarterly column “Federal Developments.” Mr. Greenblatt has also served as adjunct faculty instructor at John Marshall Law School’s LL.M. in Employee Benefits Program and is a Fellow of the American College of Employee Benefits Counsel.

Because of Mr. Greenblatt’s particular experience with respect to welfare benefit programs, Katten Muchin Zavis Rosenman serves as special-benefits counsel to many Fortune 500 companies. This work ranges from the design, documentation and implementation of employee welfare trusts to the representation of employers/trusts before the IRS and DOL on audits, ruling requests and litigation.

Jeffrey J. Bakker’s practice involves advising employers in the design, drafting and administration of qualified retirement benefit plans, nonqualified deferred compensation plans and equity-based compensation plans. His practice also includes providing assistance with the employee benefits aspects of corporate transactions.

Mr. Bakker received his law degree from the University of Illinois, where he graduated magna cum laude in 1997. He received his undergraduate degree in mathematics and government from Monmouth College, where he graduated magna cum laude in 1990.