

Deciphering the implications of HIPAA compliances

Approximately four months after HIPAA's compliance date, the acronym has become a buzzword among employers within and outside of the medical arena. Yet many professionals are still uncertain how to properly comply with HIPAA's regulations, even though failure to comply can result in civil monetary and criminal penalties.



**Jennifer
Rangel**

The Health Insurance Portability and Accountability Act, or HIPAA, has been likened to Y2K on steroids. Yet, unlike Y2K, compliance with HIPAA doesn't end on the compliance date, but instead, it's only the beginning.

HIPAA was enacted to safeguard the privacy and security of health information and to strive to improve the health care industry's efficiency and effectiveness. The act protects all health information about an individual, including a person's medical history, by putting restrictions on the information's use and disclosure outside of the individual's health plan, with certain exceptions.

Employer-sponsored health plans are subject to these new sweeping rules that change the way in which the plans handle and transmit an insured's medical information.

Most health plans, including employer-sponsored health plans, were required to be in compliance by April 14. Smaller health plans with less than \$5 million in annual receipts have until April 14, 2004, to come into compliance. For a fully insured group health plan, annual receipts are defined as annual premiums paid. For a self-insured health plan, annual receipts means total claims paid for the plan's last full fiscal year.

Though employers aren't covered entities under HIPAA, most employers sponsor a health plan, and that plan is a covered entity under HIPAA. Depending upon the degree of health information the employer — as the plan's sponsor — receives, the employer may incur obligations under HIPAA and should be aware of these responsibilities.

A sponsor of a fully insured health plan who only receives summary health information — such as an individual's claims history or claims expenses to obtain premium bids or to modify, amend or terminate the health plan — generally won't need to enact comprehensive privacy policies. Summary health information most often has been "deidentified" except for the insureds' ZIP codes. To deidentify health information, the plan must remove all iden-

tifiers such as the individual's name, address and social security number.

Sponsors also can receive information about whether an employee or dependent is enrolled in or has cancelled a health plan without incurring significant HIPAA privacy responsibilities. Many employers with fully insured plans have minimized their responsibilities further by specifying to the health insurer that they receive only deidentified health information. By this method, sponsors receive the claims history on their employees in the aggregate, but specific claims aren't associated with individual employees.

Where HIPAA responsibilities mostly come into play is with sponsors of self-insured health plans — because they play a large role in administering their plans — and sponsors of fully insured plans who receive detailed health claims information. In both of these situations, according to HIPAA, sponsors have to establish new procedures that restrict the use and disclosure of employee and dependent health information. They also must amend their summary plan descriptions to explicitly allow the plan sponsor to use and disclose health information and to identify employees of the plan who will have access to health information and who can administer the plan.

No matter the level of an employer's HIPAA responsibilities, it's the daily compliance that seems to cause the most confusion — for instance, how to handle advocacy services for employees. Under HIPAA, an employer must provide advocacy services when an employee turns to the human resources department for assistance in obtaining health coverage or for receiving reimbursement from the health plan for a medical treatment, service or product. The human resources department acts as an advocate for the employee with the health plan or the third-party administrator. According to HIPAA, the employer, acting as the plan sponsor, must either obtain an authorization from the applicable employee or dependent or amend the summary plan description to allow the plan to perform advocacy services and designate certain employees to serve as advocates for the employees.

Another area of confusion is how the HIPAA privacy rules apply to other employer programs. Although HIPAA applies to group health plans, it excludes disability plans, workers' compensation programs, life insurance plans and employee assistance plans that deal with professional referrals only. It is unclear whether HIPAA applies to medical flexible spending accounts and occupational benefit Employee Retirement Income Security Act injury plans, which

many non-subscribers to the Texas Workers' Compensation program utilize.

The federal agency responsible for enforcing HIPAA has indicated informally that a flexible spending accounts may be required to comply with HIPAA if it's qualified as an ERISA plan. ERISA occupational benefit injury plans fall into an even grayer area, because workers' compensation insurance is specifically excluded from HIPAA. Consequently, administrators of these plans argue that they should be excluded too.

Nonetheless, many large employers who sponsor FSAs are taking a precautionary approach and proceeding with implementing HIPAA compliance.

Third-party administrators, who employers sometimes contract out to handle the day-to-day operations of a health plan, are another gray area. Sponsors of self-insured health plans who use third parties may want to consider delegating many of their HIPAA responsibilities, to the extent possible, to the third party in the formal contract.

It's important for third party administrators to understand that although they may be covered by HIPAA in its own right, they also will be subject to HIPAA as a business associate or contractor of the health plan, regardless of whether the plan's sponsor formally delegates any HIPAA responsibilities to the third party.

The health plan must specify in its terms that it has entered into a contract with the third party and other business associates and requires the business associate to comply with HIPAA and the health plan's privacy procedures.

Many other areas of uncertainty have arisen since the April compliance deadline including:

- How should a health plan respond to subpoenas requesting health information?
- May divorced parents not enrolled in the plan obtain health information on their children who are enrolled?
- What health information may an enrollee's spouse receive?

We will have to wait for further guidance from the federal government on all these issues. In many cases, sponsors must refer to state law in conjunction with HIPAA to resolve these issues. For now, employers with health plans and HIPAA responsibilities may want to consult with legal counsel as they work toward daily compliance.

JENNIFER RANGEL is a partner in the Austin office of Locke Liddell & Sapp, whose practice focuses on health care issues. She can be reached at (jrangel@lockeliddell.com).

