EMPLOYER BEWARE: THE LOOMING HIPAA COMPLIANCE DEADLINE

By Adam Cantor

On April 14, 2004, the majority of employers that sponsor group health plans for their employees (those whose plans receive less than $5 million in annual premiums from the employer and the employees) will face new and extensive administrative requirements under the Health Insurance Portability and Accountability Act of 1996, the law known as HIPAA. Yes, that's right. The majority of **employers** will face these requirements, which relate to the protection of confidential medical information from improper use or disclosure.

Many employers believe that the insurers or HMOs that provide the coverage and handle the day-to-day administration of medical claims will also handle all aspects of HIPAA compliance. To put it bluntly, many employers believe that they need to do nothing to comply with the new privacy rules – they "pay" their insurers or HMOs to deal with such administrative issues.

Unfortunately, employers that take this position risk fines and penalties for non-compliance with the new rules – under HIPAA, an employer can be fined $100 for each violation, up to a maximum per year of $25,000 for all violations of the same requirement. For one thing, it is the employer, not the insurer or HMO, that serves as administrator of the group health plan. To be sure, the insurer or HMO frequently processes claims for benefits, but it is the employer that has ultimate responsibility for administering the plan. As **plan administrator**, the employer will need to use or disclose confidential medical information for at least two purposes:

- to assist employees in submitting their claims to the insurer or HMO (how many times does an employee ask the human resources department for help in dealing with the insurer or HMO providing coverage?) and

- to fulfill its fiduciary duty, under the Employee Retirement Income Security Act of 1974, the law known as ERISA, of ensuring that the insurer or HMO complies with the United States Department of Labor's new claims review procedures. (As an aside, the failure to comply with the Department of Labor's rules subjects the **employer** to civil suit, in federal court, by the affected employees.)

Moreover, it is the employer, not the insurer or HMO, that sponsors the group health plan. As **plan sponsor**, the employer will need to use or disclose confidential medical information for one or both of the following purposes:

- to re-bid coverage with a new insurer or HMO (the new carrier is likely to demand to see information on the previous year's "extraordinary" medical costs) and/or

- to amend the plan to change levels of coverage, employee premium obligations, etc.

So, what should an employer be doing **now** to ensure compliance by the April 14th deadline?

Learn about HIPAA

HIPAA is an extremely complex law, so obtaining assistance from legal counsel should be a real consideration. At its most basic, however, HIPAA prohibits the employer from using or disclosing confidential medical information other than in the following circumstances:

- disclosure to the individual about whom the confidential medical information exists;
- use or disclosure in order to carry out treatment, payment or health care operations, unless such use or disclosure involves psychotherapy notes or marketing;
- use or disclosure pursuant to a signed, dated and narrowly drafted authorization; or
- disclosure to the government (state or federal) for purposes of public health, abuse/neglect investigation, fraud prevention, etc.

Make Arrangements for Required Document Preparation

Many employers may not realize this, but HIPAA explicitly requires that the privacy requirements be added to the **plan document** and **summary plan description** for the group health plan. This, of course, begs the question of whether the employer has a plan document and summary plan description for the group health plan.

In most instances, the answer to this question is no. To be sure, in most instances, the insurer or HMO will provide a certificate of coverage and a policy booklet describing covered services, co-payments, etc. However, the combination of these documents rarely amounts to a legally compliant "plan document" under ERISA, let alone a plan document that complies with HIPAA. This may be because the insurer or HMO may approach the drafting of these documents primarily (or even exclusively) from the perspective of compliance with state insurance law requirements, not from the perspective of an employer seeking to comply with HIPAA (and ERISA).

Similarly, the insurer or HMO frequently will furnish the employer with a one or two-page "summary" of benefits. Again, it appears that the drafting many times may be done from the perspective of compliance with state insurance law requirements, not from the perspective of an employer seeking to comply, in the first instance, with ERISA's requirement of a comprehensive summary of the plan, and in the second instance, with HIPAA's requirement that the privacy rules be written into the summary plan description.

In short, an employer seeking to meet the April 14th deadline should immediately review the documents provided by the insurer or HMO and begin the process of determining their compliance with HIPAA (and ERISA).

Train Employees

HIPAA also requires that the employer train the employees who will have access to confidential medical information in the relevant aspects of HIPAA compliance. What this means for an employer right now is identifying those individuals at the human resources level or management level likely to need or have access to confidential medical information. In addition, the employer should consider retaining legal counsel to help it draft a HIPAA training and procedures manual.

Enter into Business Associate Agreements

HIPAA requires that any person or entity with which the employer deals that receives confidential medical information from the employer agree to use or disclose such information in compliance with the privacy rules. For instance, an employer might contract with a third party (other than the insurer or HMO) to administer a portion of its group health plan. In such a case, the employer would have to enter into what is known as a "business associate agreement" with the third party, under which the third party agrees to comply with HIPAA in its use or disclosure of the employer's employees' confidential medical information.

Other HIPAA Compliance Obligations

In addition to the foregoing, HIPAA requires that the employer, among other things, do the following:

- designate a privacy official and contact person responsible for receiving privacy-related complaints;
- provide a process for employees to make privacy-related complaints;
- apply appropriate sanctions against members of its workforce who fail to comply with HIPAA;
- take steps to mitigate the harmful effects of improper use or disclosure of confidential medical information;
- refrain from engaging in intimidating or retaliatory acts against employees about whom the plan has provided confidential medical information to the employer; and
- maintain compliance logs for six years of all employee complaints, requests for restrictions on the use or disclosure of confidential medical information and disclosures of such information.

Why Comply?

Well, the answer is part carrot and part stick. First, the carrot. An employer that complies will foster positive employee relations, improve the operation of its group health plan and insulate itself from the possibility of being sued under a state invasion of privacy law. (HIPAA does not

afford employees the right to sue for invasion of privacy, but state law frequently does, and in this regard, complying with HIPAA can only help the employer.)

Now the stick. As discussed above, an employer that violates HIPAA risks being fined $100 per violation, up to a maximum of $25,000 per year. Further, it is likely that serious violations of HIPAA will encourage affected employees to notify the federal Department of Health and Human Services, the agency charged with administering HIPAA, thereby increasing the likelihood of intrusive government audits. Finally, criminal penalties exist for egregious violations of HIPAA.

Adam Cantor is an associate in the Employee Benefits Practice Group of Brown Rudnick Berlack Israels (www.brownrudnick.com). Mr. Cantor specializes in the areas of ERISA, tax law, employment law, executive compensation and business succession planning.

This article was originally published by HR.com on April 5, 2004.