

LEGAL ALERT

February 2004

New Medical Privacy Rules Impact Employers and Group Health Plans

DEADLINE FOR COMPLIANCE IS APRIL 14, 2004

By: Richard C. Kraus, Rachel Brochert Roe, and Ashley W. Taylor

Many businesses are surprised to learn that new federal medical privacy rules directly impact how health information about employees may be handled. Compliance with the new rules does not apply just to health care providers and insurance companies, but also any company with an employee welfare benefit plan that provides medical care to employees or dependents – directly or indirectly, through insurance, reimbursement, or otherwise. This includes any employer that offers medical, prescription, dental or vision coverage or maintains a flexible spending account (medical reimbursement) plan.

What is HIPAA?

As part of the federal Health Insurance Portability and Accountability Act (HIPAA) enacted in 1996, Congress directed the Department of Health and Human Services to disseminate regulations to standardize electronic health care transactions and to protect the privacy and security of information relating to an individual's medical history, condition and treatment. The regulations that address the privacy of individual health information went into effect in 2003 and cover all health care providers, health care clearinghouses, and group health plans. Most health care providers and insurers were to be compliant with these privacy regulations by April 14, 2003. For many small to mid-size businesses that provide health care benefits to employees, compliance will be required by April 14, 2004.

How are employers affected by the federal medical privacy rules?

Employers may wear three different hats when dealing with employees and their health information. First, a company acts as the employer. Second, the employer is the "plan sponsor" of the benefit programs offered to employees. Third, the employer is a "group health plan" that directly or indirectly provides the benefits.

When dealing with employees on typical work-related issues, i.e. when acting as the employer, employers are not directly affected by HIPAA. An employer can use health-related information about employees for employment related purposes, such as pre-employment screening, fitness for duty, disability, sick time, and similar matters, without being regulated by HIPAA. (Employers must be conscious of other laws that might apply such as the Americans with Disabilities Act, Family Medical Leave Act, and various statutes relating to mental health and substance abuse.)

HIPAA may, however, affect how employers can obtain health information from providers and from insurers. As discussed later in this Alert, it will also restrict how information can be acquired from an employer's own health plan.

As mentioned, businesses providing health benefits to employees also act as the "plan sponsor" of a "group health plan." The "plan sponsor" establishes and maintains the employee benefit plan. The "group health plan" provides or pays for benefits to employees by obtaining insurance, contracting with HMOs and provider organizations, reimbursing employees, paying premiums, or by self-insuring.

Although a group health plan is a separate legal entity from the employer/plan sponsor, most plans are not separate in their practical operation. Often the only tangible evidence of the existence of a group health plan is the contractual agreement that describes the rights and responsibilities of covered participants, including the benefits that are offered and the eligible recipients. These are referred to as the "plan documents." Plan sponsors are not directly subject to HIPAA. Group health plans are.

Although HIPAA only applies to the actual "group health plan" and not the sponsor/employer, the employer may perform certain functions that are integrally related or similar to the functions of group health plans. In carrying out these functions, the employer may require access to individual health information held by the group health plan. HIPAA places restrictions on the flow of information from the group health plan to the employer.

Continued on back

The rule seeks to ensure that employers who receive protected health information from the health plan only use that information for the administration of the health plan and not for other employment-related purposes, such as hiring and firing decisions. The degree of HIPAA's impact on an employer as a sponsor will therefore greatly depend on its need to receive and use protected health information from the health plan to perform plan administrative functions.

What needs to be done for HIPAA compliance?

While the specific requirements for HIPAA compliance are not covered in this Alert, there are general approaches and principles that should be followed. The first step is to determine if and to what extent HIPAA applies to a business. An employer needs to analyze whether and how protected health information is received by the employer in connection with its group health plans. To the extent that the employer receives protected health information, other than summary health information or enrollment/disenrollment information, it will need to amend its plan documents to permit the receipt and use of such information. The group health plan offered by the employer may also need to develop appropriate policies and procedures to safeguard protected health information and implement the administrative requirements under HIPAA.

For example, if the group health plan offered by the employer is a self-insured plan, including a flexible spending account (FSA) or a stand-alone dental or vision plan, the employer will most likely have access to protected health information for administrative purposes, including claim appeals and audits. The privacy rule will have a much greater impact on the group health plan in this case.

This type of group health plan should amend its plan documents to limit the sponsor's use of protected health information to plan administrative purposes only and identify the members of the sponsor's workforce that will have access to the protected health information. In addition, the group health plan

should appoint a privacy officer to oversee compliance efforts, including the adoption of policies and procedures that safeguard protected health information and that address an individual's rights with respect to their protected health information. The group health plan should also develop notice of privacy practices and conduct privacy training of its workforce.

On the other hand, group health plans that provide benefits only through an insurance contract and that do not create, maintain, or receive protected health information (i.e. fully insured plans) do not have to meet many of the administrative responsibilities under HIPAA. These requirements are satisfied by the health insurance issuer or HMO that is providing the benefits under the group health plan. For example, the group health plan does not have to deliver a notice of privacy practices to the enrolled employees.

Employers may also engage the services of third parties to assist them in the administration of the group health plans, such as third party administrators, attorneys, or accountants. If the group health plan discloses protected health information to these third parties who provide services on its behalf, they are considered "business associates" of the group health plan under HIPAA.

Before the group health plan can disclose protected health information to a business associate, such as a third party administrator, it should obtain satisfactory assurances that the business associate will properly safeguard the information. This is done through a business associate agreement, which contains certain provisions that require the business associate to comply with HIPAA.

When must a business be in compliance?

The deadline for complying with the privacy rule was April 14, 2003. There is a provision in HIPAA, however, that gives "small health plans" an additional year, until April 14, 2004, to comply with HIPAA's privacy requirements.

"Small health plans" are defined as a health plan with "annual receipts" of \$5 million or less. Fully insured health plans should use the amount of total premiums that they paid for health insurance benefits during the plan's last full fiscal year to determine their annual receipts. Self-insured plans, both funded and unfunded, should use the total amount paid for health care claims by the employer during the plan's last full fiscal year.

Why should a business care about HIPAA?

A violation of HIPAA can result in significant civil and criminal penalties (up to \$250,000 in fines and 10 years imprisonment). There is also a risk of civil liability. Lawsuits for violating an individual's privacy rights are becoming very common. Because of HIPAA, employees are much more conscious of their privacy rights relating to medical information. They will expect the same level of protection from their employers.

If you have any questions about HIPAA's impact on businesses or would like assistance in evaluating your own group health plan, please contact our HIPAA compliance team. We can tailor our HIPAA Group Health Plan Compliance Kit to meet your organization's needs.

The Members of
**SMITH HAUGHEY
RICE & ROEGGE'S**
HIPAA Compliance Team are:

R. Jay Hardin	231.486.4534 <i>Traverse City</i>
Richard C. Kraus	517.318.5653 <i>East Lansing</i>
Christopher R. Genther	616.458.0222 <i>Grand Rapids</i>
Veronica A. Marsich	734.913.6661 <i>Ann Arbor</i>
Rachel Brochert Roe	231.486.4503 <i>Traverse City</i>
Ashley W. Taylor	734.913.6907 <i>Ann Arbor</i>
