

Client Special Briefing

Special Legal News • June 2003

How To Comply with Privacy Rule of HIPAA

Patricia F. Weisberg

Employers that sponsor health plans face another new challenge from the privacy provisions of the Health Insurance Portability and Accountability Act ("HIPAA"). HIPAA was signed into law in August 1996 during Clinton's presidency. The law was originally intended to provide access to health insurance, increase protection of health information and to reduce administrative costs. While the goal of protecting the privacy of employees is noble, what it means for you is more work. In order to comply with the privacy rule of HIPAA, you need to carefully analyze of the structure of your existing benefit plan and then make some decisions on how best to proceed. This special client briefing outlines how the privacy rule could apply to you, and gives general direction on how to bring your company up to speed.

Most companies covered by HIPAA should have complied with the privacy rule by April 14, 2003. "Small" health plans - defined as those having annual receipts of 5 million or less - have an extra year to comply. The privacy rule applies to:

- Health plans (HMO's, health insurance companies, group health plans which includes vision and dental, flexible spending, and employee assistance plans that provide for health care)
- Health care clearing houses (i.e., billing companies);
- Health care providers who transmit any health information in electronic form

While employers are not covered entities under HIPAA, employer sponsored health plans are (with some exceptions). The law included employer sponsored health plans under HIPAA to prevent employers from using employees' personal health information when making employment-related decisions. The employer-sponsored benefit plans that HIPAA covers are:

- Any group health plan with 50 or more participants (employees or former employees; not dependents)
- Any group health plan administered by any entity other than the plan sponsor (ie. third party administrator).

Basically, the only way an employer-sponsored benefit plan is not covered is if the plan is self-administered and there are less than 49 participants. This will be true only in very rare occasions. There are employee sponsored benefit plans that do not meet the definition of "group health plan" under HIPAA. These include life insurance, death benefits, and disability and workers' compensation.

Employers that sponsor benefit plans must comply with HIPAA privacy rules. The law requires employers to distinguish between

their human resource functions and their functions as plan sponsors. Human resource functions include such things as hiring, firing and administration of employment laws such as FMLA, ADA, leaves of absence, and workers' compensation, etc. Employer functions as "plan sponsors" include such things as:

- Establishing, amending and terminating plans
- Performing enrollment and disenrollment functions
- Obtaining insurance premium bids.

Health information that the employer receives about its employees in order to administrate its employment-related policies other than the administration of the health plan is not what HIPAA calls "PHI" or protected health information. Employers, therefore, will need to maintain three different files on each employee - a personnel file, a personnel/health information file, and a health information/HIPAA file. The only health information that the employer should maintain in the HIPAA file is information the employer received while functioning as the health plan sponsor.

Employers that play an active role in the management of a health plan, or employers who sponsor self-insured group health plans will need to comply with more requirements than employers whose plans are insured by a third-party carrier and who also choose not to perform any administrative functions for the group health plans. A plan sponsor's obligation under the privacy rules will vary depending upon whether the plan sponsor (i.e., employer) receives protected health information, summary health information, or no health information.

Protected health information (PHI) is individually identifiable health information that is transmitted by electronic media, maintained in any electronic media, or transmitted or maintained in any other form or medium. In its definition of protected health information, the law specifically excludes employment records held by a covered entity in its role as employer. Generally the information is covered by the HIPAA privacy rules if it:

- Identifies an individual
- Is created or received by a covered entity, including employer sponsors
- Relates to the past, present, or future physical or mental condition of an individual, provision of health care to an individual, or payment for the provision of health care to an individual

Unprotected information is called de-identified information. Information is de-identified if it does not include such things name,

address, admission date, birth date (generally), telephone and fax numbers, electronic mail address, social security number, medical records numbers, health plan beneficiary numbers, account number, certificate/license numbers, vehicle identifiers and serial numbers, device identifiers and serial numbers, internet protocol (IP addresses), web universal resource locators (URL's), bi-metric identifiers, including finger and voice prints, photographs or images, and any other unique identifying number, characteristic or code.

Employers that are plan sponsors may choose to receive summary health information in lieu of PHI. Summary health information is information that may be individually identifiable health information:

- That summarizes the claim's history, claim's expenses, or type of claim's experiences by individuals for whom a plan sponsor has provided health benefits under a group health plan
- From which the individually identifiable information has been deleted
- Is used for (1) obtaining premium bids for providing health information coverage to the group health plan; or (2) modifying, amending or terminating the group health plan.

For employers that do not have a need for more detailed information, the easy answer is for the employer to make sure it receives only summary health information. But this means that an employer cannot then act as an administrator of the health plan. Administration includes payment and "health care operations." The law defines administrative activities as having information regarding eligibility and coverage determinations, claims adjudications, risk adjustment, coordination of benefits, claim's management, billing and obtaining payment. In most cases, the administrative type work an employer sponsor typically performs is assisting its employees when there is a problem or issue with respect to coverage or payment for certain services. For example, an employee may give the employer what is typically called an "Explanation of Benefits" or EOB form. An employer might then assist the employee by calling the health care provider or insurance company to find out what the problem is and try to get the bill paid. This throws the employer into the category of administrator and greatly increases the obligation imposed on the employer sponsor.

Plan sponsors that offer a self-funded group health plan and as a result perform administrative functions and receive more than summary health information must fully comply with HIPAA. This means that they must:


- Amend group health plan documents
- Provide certification to group health plan that it amended plan documents
- Name privacy official
- Designate a contact person
- Train all workforce members (temps and volunteers included)
- Establish administrative, technical and physical safeguards, complaint procedures, sanctions policy, litigation policy, non-retaliation policy, non-waiver of rights policy, documentation and retention policy and

methodology, and other necessary procedures required to implement the privacy safeguards

Plan sponsors that are self-funded group health plans that do not perform administrative functions and that receive only summary health information must also comply with all of the above requirements, except that these plan sponsors do not have to amend plan documents or provide certification.

Plan sponsors that receive only summary health information and do not perform administrative functions do not have to amend plan documents, provide certification or comply with other requirements listed above. They do, however, have to establish a non-waiver of rights policy and establish a non-retaliation policy. Plan sponsors, however, that offer fully-insured group health plans but also perform administrative functions have basically the same obligations as those who are self-funded.

As an employer plan sponsor, you must decide where you fit. Do you offer a self-insured plan? Do you offer solely a plan insured by a third-party carrier? Do you offer reimbursement to your employees for health care expenses and what type of information must the employee provide to you? What type of health information do you receive about your employees? Do you perform any administrative functions? Once you have determined your current situation, you may want to reevaluate whether you wish to be involved in the overall management and administration of the group health plan. If you, as the plan sponsor, decide that you must receive or use PHI, then you will need to formulate a plan and reach compliance with all of the HIPAA privacy regulations. If, however, you determine you do not need to receive PHI and that it is not necessary for you to perform administrative functions, your obligations will be greatly decreased. Many employer plan sponsors who use a broker to assist in purchasing health insurance may opt to delegate the administrative responsibilities to the broker. You can avoid many obligations under the HIPAA privacy rules by delegating the administrative functions. Each employer plan sponsor will need to evaluate whether the receipt of PHI is necessary and whether it benefits the employer in some way to assist in the administration of the plan. Benefits to the employer may be measured in a variety of ways (i.e. measured in terms of economics or employee morale).

HIPAA's goal is to insure that employers do not improperly use personal health information. Keep in mind that while the law expressly clarifies that an employer is not a covered entity, by covering "group health plans" most employee welfare benefit plans providing benefits to employees pursuant to ERISA are covered by the regulation. Employers that decide to play an active role in the management of their health plan, including self-insured plans, will need to meet a major compliance obligation. For those employers that decide they do not need PHI and do not need to perform administrative tasks will be able to avoid many of the obligations imposed by the HIPAA privacy rule. 

For more information on this or other employment law matters, please feel free to contact our Employment Law attorneys:

Michael McMenamain (mmcmenamain@walterhav.com) 216-928-2929

Nancy A. Noall (nnoall@walterhav.com) 216-928-2926

Patricia F. Weisberg (pweisberg@walterhav.com) 216-928-2928

Patricia J. Haas (phaas@walterhav.com) 216-928-2892

Susan M. Zidek (szidek@walterhav.com) 216-928-2936

Randal G. Ammons (rammons@walterhav.com) 216-928-2932

Morris L. Hawk (mhawk@walterhav.com) 216-619-7842

Prefer E-Mail?
To receive future Client Briefings via e-mail, please
send your e-mail address to
ctalbert@walterhav.com
Change of Address?
Write Client Briefing, W&H, 1300 Terminal Tower,
50 Public Square, Cleveland, OH 44113-2253

©2003 Walter & Haverfield LLP All rights reserved.
The information in this newsletter is a summary of often
complex legal issues and may not cover all the "fine points"
related to a specific situation or court jurisdiction.
Accordingly, it is not intended to be legal advice, which
should always be obtained in consultation with an attorney.

WALTER & HAVERFIELD LLP
Attorneys at Law

1300 Terminal Tower ■ 50 Public Square ■ Cleveland, Ohio 44113-2253

Tel: 216-781-1212 ■ Fax: 216-575-0911

www.walterhav.com