VEDDER PRICE

# HIPAA Bulletin

February 2003

## HIPAA PRIVACY RULE AND EMPLOYERS

On August 14, 2002, the Department of Health and Human Services issued the final privacy regulation under the Health Insurance Portability and Accountability Act ("HIPAA"), generally referred to as the "Privacy Rule." The Privacy Rule restricts the use of protected health information by various organizations (referred to as "covered entities"), including group health plans. As a covered entity, a group health plan may not use or disclose protected health information for purposes unrelated to the provision of health benefits without first receiving written authorization to do so from the subject individual, unless otherwise permitted or required under law.

Protected health information ("PHI") is defined as individually identifiable health information, transmitted or maintained in any medium, that relates to an individual's past, present or future physical or mental health. PHI is considered "individually identifiable" if it identifies an individual or contains enough specific information to render it identifiable. PHI generally falls into one of three categories:

1. information relating to a previous health condition, a chronic illness, or a propensity for a certain disease;

2. information relating to health care treatment an individual has received, is receiving or will receive; or

3. information relating to the payment for health care services an individual has received, is receiving or will receive. It is important to recognize that PHI does not need to be in writing to be protected; oral information also is protected.

Although employers are not identified as covered entities, they undertake certain obligations and responsibilities under the Privacy Rule by virtue of their status as plan sponsors. The scope of these responsibilities will vary depending on the functions the employer performs on behalf of the group health plan. For example, if an employer performs activities related to the plan operations, such as providing claims assistance, quality assurance, auditing, monitoring, management, claims processing and payment (referred to as "plan administration functions"), as opposed to merely assisting the group health plan with enrollment and disenrollment activities (referred to as "plan sponsor functions"), the employer will assume more significant compliance responsibilities.

### *Use or Disclosure of Health Information by a Group Health Plan*

As a covered entity, a group health plan is subject to certain restrictions on uses and disclosures of PHI. A group health plan may use and/or disclose PHI for limited purposes without obtaining prior consent from the individuals who are the subject of the health information. These purposes include: to conduct payment activities and health care operations; to respond to a court order or a valid subpoena; and limited public policy purposes.

All other uses and/or disclosures of PHI must be accompanied by a valid authorization. In order to be valid, an authorization must include nine elements:

- ✓ a reasonably specific description of the PHI to be used or disclosed;
- ✓ the name of the person (or job title of person) authorized to make the requested use or disclosure;
- ✓ the name of the person (or job title of person) permitted to receive the information;
- ✓ a reasonably specific description of the purpose of the use or disclosure;
- ✓ an expiration date or expiration event;
- ✓ a statement of the individual's right to revoke the authorization and an explanation of the revocation procedure;
- ✓ an explanation of the consequences (if any) of the individual's failure to provide the authorization;
- ✓ a statement that the information disclosed may be redisclosed to an individual or entity that is not subject to the Privacy Rule and no longer protected; and
- ✓ the individual's signature.

The Privacy Rule permits a group health plan to share PHI with its plan sponsor without first obtaining an individual authorization in order to assist the sponsor with certain responsibilities associated with plan sponsor functions. For example, a group health plan may disclose PHI for enrollment or disenrollment purposes. Similarly, a group health plan may disclose summary information that contains identifiers in connection with amending group health plan documents or obtaining premium bids from other health plans or to provide information about the general health of the individuals enrolled in the health plan in order to determine whether it is necessary to add additional covered services.

A group health plan may disclose PHI to the plan sponsor for any purpose related to plan administration only after the plan sponsor has certified that it will act in accordance with the terms of the Privacy Rule and has amended its plan document to restrict uses and disclosures of PHI by the plan sponsor as required by the Privacy Rule.

**Administrative and Technical Requirements**

*Privacy Notice.* The group health plan must create a Privacy Notice, which provides an explanation of the uses and disclosures of PHI that the group health plan will make. The Privacy Notice identifies the individual's rights and the plan's legal duties with respect to the PHI, and includes examples of anticipated uses and disclosures of PHI. The Privacy Rule contains specific rules pertaining to the substance of the Privacy Notice, requiring that all Privacy Notices be written in plain English and follow a designated format.

*Individual Rights.* The group health plan must afford all employees and their dependents certain rights created by the Privacy Rule. All individuals must have a right to access and copy their PHI that is in the possession of the group health plan. The group health plan must give all individuals a right to request amendments to their PHI, but such requests need not be honored. All individuals have a right to receive an accounting of disclosures of their PHI made by the health plan during the previous six years, except that the group health plan need not provide an accounting of disclosures made prior to April 14, 2003.

*Privacy Official and Contact Person.* The group health plan must designate an individual who will be responsible for developing and implementing the plan's privacy and procedures policies. The group health plan also must identify a contact person to receive complaints and provide information about the plan's privacy practices. These positions need not be held by the same individual.

*Policies and Procedures.* The group health plan must create and implement policies and procedures designed to safeguard the privacy and security of PHI in compliance with the Privacy Rule. The scope of the policies and procedures will vary among plans but should address the various requirements set forth in the Privacy Rule and how the group health plan anticipates responding to them. For example, the group health plan must create and apply a policy intended to mitigate harmful effects of improper uses and disclosures of PHI. Similarly, a group health plan must have in place a nonretaliation policy that clearly provides that it will not take retaliatory action against an individual who exercises his or her rights under the Privacy Rule or against an employee who refuses to participate in a practice that is in violation of the Privacy Rule. Moreover, a group health plan may not require a plan participant to waive his or her rights to report violations or suspected violations of the Privacy Rule to the Department of Health and Human Services as a condition to participating in the plan.

After the policies and procedures are created and implemented, the group health plan must develop a disciplinary policy applicable to inappropriate uses and disclosures of PHI by employees who work with the plan or by employees who access PHI that has been disclosed by the plan. All violations of this policy must be documented and maintained by the group health plan for at least six years.

*Employee Training.* All employees who work with the group health plan, and those who do not work with the plan but will receive PHI from it, must be trained on the policies and procedures relating to proper handling of PHI. All current employees must be trained before April 14, 2003. Training of new employees must occur within a "reasonable period" of time after joining the workforce.

*Amendments to Plan Documents.* If the employer, as plan sponsor, will use PHI to perform plan administration functions, it must amend its plan documents to indicate the employer's agreement to certain restrictions on its use and/or disclosure of PHI. Only certain employees (or classes of employees) identified in the plan documents will have access to PHI. These individuals may use and/or disclose PHI only for the limited purposes of plan administration, as specifically described in the plan documents, or as required by law. All agents or subcontractors of the employer who received PHI from or on behalf of the employer will agree to the same restrictions imposed on the plan sponsor. Finally, the employer must agree not to use PHI received from the group health plan for employment-related decisions.

In addition to amending the plan documents, the employer must assume certain responsibilities relating to the security and privacy of PHI. Among these responsibilities is an obligation to ensure adequate separation between the employees who are involved in group health plan activities and those who are not. The employer must afford employees and dependents the right to review and amend any PHI that the employer has in its control and document all disclosures of PHI. Upon request of the group health plan, the employer must provide an accounting of disclosures to the group health plan upon request.

***Compliance Responsibility Baskets***

The scope of an employer's responsibilities under the Privacy Rule varies depending on the employer's level of involvement in the administration of the group health plan it sponsors. In an effort to simplify the determination, it is helpful to conceptualize different "compliance baskets" full of administrative and technical responsibilities. Which basket an employer carries depends on the level of involvement in the group health plan activities the employer desires.

### Basket #1

This basket is carried by employers that sponsor self-funded group health plans, receive only summary information and do not perform plan administrative functions. The employer does not need to amend its plan documents because it will only perform plan sponsor functions. The employer must, however, comply with all of the administrative requirements and provide plan participants with individual rights with respect to their PHI.

The employer must distribute a Privacy Notice to all employees then enrolled in the group health plan on or before April 14, 2003. All employees participating in the plan after April 14, 2003 must receive a copy of the Privacy Notice at the time of enrollment.

### Basket #2

This basket is carried by employers that sponsor self-insured group health plans and perform plan administration functions. For example, these employers might assist their employees with filing claims or conduct a review of denied claims. In this situation, the employer must amend its plan documents to permit the disclosure of PHI from the group health plan to the employer for plan administration purposes and certify to the group health plan that it will use PHI only in accordance with the terms of the Privacy Rule. The employer must comply with all of the administrative requirements and provide the plan participants with their individual rights with respect to PHI.

The employer must distribute a Privacy Notice to all employees then enrolled in the group health plan on or before April 14, 2003. All employees participating in the plan after April 14, 2003 must receive a copy of the Privacy Notice at the time of enrollment.

### Basket #3

This basket is carried by employers that sponsor fully insured group health plans, receive only summary information, and do not perform plan administration functions. This is the least full of all baskets.

The employer does not need to amend its plan documents or provide a certification to its health insurer or HMO because it will only receive health information in summary form. The employer must comply with only two administrative requirements:

(i) adopt a policy providing that it will not require participants to waive their rights; and
(ii) adopt a policy providing that it will not retaliate against individuals who exercise their rights.

The employer does not need to create and distribute a Privacy Notice or take any action to ensure that the health plan participants can exercise their rights with respect to their PHI under the Privacy Rule because the health insurer or HMO will assume this responsibility.

### Basket #4

This basket is carried by employers that sponsor fully insured group health plans that perform plan administration functions. The employer must amend its Plan Documents and provide a certification to its health insurer or HMO because it will receive PHI from the group health plan. The employer must comply with all of the administrative requirements and provide the plan participants with their individual rights with respect to PHI.

The employer must create and maintain a Privacy Notice but need only provide it to a plan participant upon request. The health insurer or HMO will create and distribute a separate Privacy Notice to plan participants.

***Conclusion***

Employers will assume significant responsibilities under the Privacy Rule by virtue of the group health plans they sponsor. There is quite a lot to do before April 14, 2003 (or a year later for small health plans). Employers should begin to structure a compliance strategy to ensure that everything is in place prior to the compliance date.

## VEDDER, PRICE, KAUFMAN & KAMMHOLZ

### About Vedder Price

Vedder, Price, Kaufman & Kammholz is a national, full-service law firm with approximately 200 attorneys in Chicago, New York City and Livingston, New Jersey.

Vedder, Price, Kaufman & Kammholz
(A Partnership Including Vedder, Price, Kaufman & Kammholz, P.C.)

*Chicago*
222 North LaSalle Street
Chicago, Illinois 60601
312/609-7500
Fax: 312/609-5005

*New York*
805 Third Avenue
New York, New York 10022
212/407-7700
Fax: 212/407-7799

*New Jersey*
354 Eisenhower Parkway, Plaza II
Livingston, New Jersey 07039
973/597-1100
Fax: 973/597-9607

www.vedderprice.com

### About the Vedder Price HIPAA Task Force

Earlier this year, Vedder Price assembled a multidisciplinary HIPAA Task Force, comprising members of the Health Law and Employee Benefits Practice Groups, to provide guidance to clients affected by the recently finalized Privacy Rule implementing certain aspects of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The attorneys serving on the HIPAA Task Force have substantial experience representing a broad range of clients regarding health law, employment law and employee benefits issues. This experience and perspective enables Vedder Price to provide strategic advice and practical guidance to health providers, insurers and employers regarding the new responsibilities and challenges created by HIPAA and its regulations pertaining to the privacy and security of health information.

### Principal Members of the HIPAA Task Force

| | |
|---|---|
| Richard H. Sanders | 312/609-7644 |
| Paul F. Russell | 312/609-7740 |
| John J. Jacobsen, Jr. | 312/609-7680 |
| Neal I. Korval (New York) | 212/407-7780 |
| Philip L. Mowery | 312/609-7642 |
| Kathryn L. Stevens | 312/609-7803 |
| William T. Daniels | 312/609-7508 |
| Karen N. Brandon | 312/609-7732 |
| Christopher T. Collins | 312/609-7706 |