

## Employer Compliance with HIPAA's Privacy Rules

In connection with implementing the protected privacy requirements of the Health Insurance Portability and Accountability Act (“HIPAA”), the Department of Health and Human Services (“HHS”) issued extensive regulations aimed at protecting individuals’ health care privacy (“Privacy Rules”). Under the Privacy Rules, “Covered Entities” may not use or disclose individually identifiable health information, which is referred to as “Protected Health Information,” unless the appropriate form of permission has been obtained from the individual or the use or disclosure is expressly allowed by HIPAA. “Covered Entities” include group health plans, health care providers and health care clearinghouses. This memorandum examines the application of the Privacy Rules to group health plans only (which would include medical plans as well as cafeteria plans that include medical reimbursement accounts), and particularly the impact of the new rules on employers who sponsor such plans. (Self-insured plans that are self-administered and cover fewer than 50 participants are exempt from the Privacy Rules.)

For other than “Small Health Plans”, the Privacy Rules are effective April 14, 2003. Small Health Plans, which are those having “annual receipts of \$5 million or less” (a parameter that has not yet been further defined) have until April 14, 2004 to comply.

**It is imperative that any employer who sponsors a group health plan immediately begin examining how the Privacy Rules will affect them and implementing the necessary documentation and procedures to comply with the new Rules.**

### Summary Analysis of Privacy Rule Requirements

The following summary outline should assist employers in evaluating how they may be impacted by the Privacy Rules. Following the outline is a more extensive discussion of the Privacy Rule requirements and their application to employers and their group health plans. Employers who sponsor group health plans should consider the following:

- (1) Is the employer’s group health plan self-insured or does the employer need to receive **Protected Health Information** other than just **Summary Health Information** (See part 1 below)?
  - If the answer to either question is yes, then the employer must comply with all of the Privacy Rule requirements described in the **Procedural Requirements** (See part 2 below).
  - If the answer to both questions is no, then the employer is subject to only the **Limited Procedural Requirements** (See part 2 below).

- (2) Does the employer receive **Protected Health Information** other than just **Summary Health Information**?
- If the answer to this question is yes, but the employer will not obtain a **valid authorization** from all affected individuals (See part 1.c. below), then the employer must amend all of its plans according to the **Required Amendments** (See part 1.a. below).
- (3) Does the plan or employer have contracts with any **Business Associates** (See part 3 below)?
- If the answer is yes, then such contracts will need to be revised as necessary to comply with the **Business Associate Requirements** (See part 3 below).
  - A quick-reference chart summarizing all of the Privacy Rule requirements is attached at the end of this Memorandum.

## Discussion

An employer who sponsors a group health plan will be impacted by the Privacy Rules' requirements: (1) as the sponsor of the plan to the extent the employer receives "**protected health information**" about plan participants, (2) for the plan itself if the plan is self-insured or the employer is actively involved in the management of the plan, and (3) to the extent the employer or plan contracts with outside entities (referred to as "**Business Associates**") in connection with running the plan.

### 1. Employers who Receive Protected Health Information

If an employer receives "**protected health information**" ("**PHI**") with respect to plan participants, the employer will be subject to most of the extensive requirements of the Privacy Rules. PHI is generally any health information that is (1) created or received by a Covered Entity; (2) relates to an individual's physical or mental health condition, the provision of health care to an individual or the payment for the provision of health care to an individual; and (3) identifies the individual or creates a reasonable basis to believe that the information, including demographic information, can be used to identify the individual.

#### a. Required Amendments

An employer who receives PHI in connection with managing a group health plan will either have to have a "**valid authorization**" from the individual, or will need to amend the plan documents to incorporate the following specific provisions. Specifically, the employer must agree to ("**Required Amendments**"):

- (1) Disclose PHI only as permitted by law;
- (2) Not use or disclose PHI for employment-related actions or decisions, or in connection with any other benefit or employee benefit plan of the employer;
- (3) Ensure that "adequate separation" of records and employees is established and maintained between the group health plan and the employer;

- (4) Describe and restrict access to and use of PHI to the specific class of employees under the control of the employer that will be allowed access to the PHI disclosed by the group health plan (e.g., auditors, accountants and benefits personnel);
- (5) Report any improper use or disclosure of PHI to the group health plan, and include an effective mechanism for resolving issues of improper access or use of PHI by the identified employees or other individuals;
- (6) Allow individuals to inspect, obtain copies of, and amend PHI about themselves;
- (7) Provide individuals with an accounting of disclosures of PHI made within the six years prior to the request for such accounting; and
- (8) Make its internal practices, books and records relating to the use and disclosure of PHI available to HHS for purposes of auditing the group health plan's compliance with the Privacy Rules.

**b. Exception for Summary Health Information**

Subject to the plan requirements described in Part 2 below, an employer can limit the extent to which it must comply with the foregoing Required Amendments if it does not need to receive PHI. This exception can also apply if the employer's receipt of information is limited to **"Summary Health Information"**, which is generally PHI that summarizes claims history or experience and has been stripped of specified personal identifiers. It should be noted, however, that in order to be sufficiently stripped of identifiable health information as currently required under the Privacy Rules, it would appear that any remaining Summary Health Information would most likely be of no real value at all.

**c. Exception for Valid Authorizations**

An employer may, alternatively, obtain PHI from a plan (including any insurers) without complying with the Required Amendments, if it obtains a **"valid authorization"** from the individual. A valid authorization must contain at least the following elements:

- (1) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
- (2) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
- (3) The name or other specific identification of the person(s), or class of persons, to whom the plan may make the requested use or disclosure;
- (4) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;
- (5) A statement and explanation of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke;

- (6) A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule;
- (7) Signature of the individual and date; and
- (8) If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual.

HHS has published a model form of authorization.

Thus, an employer who requires PHI in only limited instances (e.g., to assist an employee with a specific claim dispute) may choose to obtain a valid authorization from the individual to avoid complying with the burdensome Required Amendments. However, because of the detailed nature of every authorization needed, an employer who requires substantial PHI on an ongoing basis would most likely find it impractical to obtain valid authorizations from each individual for each use or disclosure of PHI.

## 2. Plan Requirements

The Privacy Rules contain extensive requirements for group health plans (unless they are exempt as discussed below) that may also impact the employers that sponsor those plans. Specifically, the Privacy Rules require group health plans to (**"Procedural Requirements"**):

- (1) **Adopt clear, written privacy procedures to protect PHI and track disclosures.** The plan must establish administrative, technical, and physical safeguards to protect the privacy of PHI to avoid intentional and unintentional prohibited uses/disclosures;
- (2) **Distribute a "Notice of Privacy Policies" to participants to communicate its privacy policies and procedures.** Among other requirements, the policy must be written in plain language, describe the uses and disclosures of PHI that are allowed for "payment, treatment and health care operations," and inform participants of their privacy rights;
- (3) **Fulfill administrative responsibilities,** which requires that the plan:
  - (i) **Designate a privacy official.** This privacy official will be responsible for ensuring that adequate privacy procedures are adopted and followed;
  - (ii) **Train employees so that they understand the privacy procedures.** This training must be provided initially by the time the health plan must be in compliance with the HIPAA privacy rules (April 14, 2003, or April 14, 2004 for small plans). An ongoing training program must be in place to address the training of new hires or changes in privacy laws;
  - (iii) **Establish grievance procedures and sanctions for privacy rights violations.** The plan must provide a way for participants to file complaints with a designated contact person about privacy policies and procedures. All complaints received and their disposition, if any, must be documented; and

(iv) **Make available to HHS the internal practices, books and records relating the use and disclosure of PHI.**

(4) **Mitigate any known harmful effect resulting from a violation of its policies and procedures about which it has knowledge.**

A plan is exempt from the foregoing requirements only if it is (1) a fully insured plan (i.e., not self-insured in any respect), and (2) the plan does not receive, use or disclose PHI other than summary health information or information on whether the individual is participating in the plan or is enrolled or has dis-enrolled from an insurer or HMO. For plans that meet these two criteria, the Privacy Rules require only that they (**“Limited Procedural Requirements”**):

- i. refrain from retaliating against individuals who are exercising their rights under the Privacy Rule, and
- ii. refrain from requiring an individual to waive his or her rights under the Rules as a condition of receiving treatment or payment or enrolling in the plan or becoming eligible for benefits.

(Plans subject to the general Procedural Requirements are also subject to the Limited Procedural Requirements.)

### **3. Business Associate Requirements**

In addition to the above requirements, group health plans and employers must negotiate or revise any written contracts with **“Business Associates”** to incorporate specific language defining the responsibilities of each party to comply with the Privacy Rules. Business Associates are persons to whom the plan or employer discloses PHI so that the persons can carry out or assist with the performance of a function for the plan or employer, and include claims processing and administration firms, utilization review and quality assurance firms, HMOs, managed care providers, billing companies, firms providing data analysis, actuarial firms, legal and accounting firms, accreditation organizations, and financial services firms. (Members of the health plan’s workforce, such as claims administrators employed by the employer sponsoring the health plan, are not considered Business Associates). All contracts with Business Associates must (**“Business Associate Requirements”**):

- (1) Establish specific permitted and required uses and disclosures of PHI by the Business Associate;
- (2) Prohibit the Business Associate from using or disclosing PHI other than as stated in the contract or as required by law;
- (3) Require the Business Associate to use appropriate safeguards for PHI;
- (4) Require the Business Associate to ensure that any agents to whom it provides PHI abide by the Privacy Rules, and report any violations to the plan;
- (5) Require the Business Associate to give participants access to their PHI, and to amend it upon request (or explain why a requested amendment is denied);

- (6) Require the Business Associate to make available the information required to provide a participant an accounting of disclosures of his or her PHI (other than disclosures for treatment purposes);
- (7) Require the Business Associate to make available its internal practices, books and records relating to the use and disclosure of PHI;
- (8) Require the Business Associate to destroy all copies of PHI when the contract terminates or, if this is not feasible, to limit further uses and disclosures; and
- (9) Authorize termination of the contract in case of a material breach of these standards.

Apart from fiduciary obligations under ERISA, an employer or plan administrator is not required to monitor the Business Associate’s performance. However, it must take action to cure material breaches when informed that they have occurred.

**4. Effect of State Laws**

The Privacy Rules do not preempt state laws that are more stringent than the federal privacy protections. Many states currently have such laws or may enact them in response to the HIPAA Privacy Rules. As a result, self-insured health plans that were not ordinarily covered by state restrictions due to ERISA preemption will now need to carefully monitor state privacy law developments as well.

**5. Penalties**

Health plans that do not comply with the Privacy Rules face penalties of up to \$100 per violation, up to an annual maximum of \$25,000 per person, for each requirement or prohibition violated. Criminal penalties are up to \$50,000 and one year in prison for knowingly disclosing PHI; up to \$100,000 and up to five years in prison if the disclosure is under “false pretenses”; and up to \$250,000 and up to 10 years in prison for if the disclosure is for commercial advantage.

If you would like further information on the Privacy Rule requirements or assistance in examining your plan(s) and bringing them into compliance with the new Rules, please contact:

<b>David E. Barry</b>	(212) 808-7618	<a href="mailto:dbarry@kelleydrye.com">dbarry@kelleydrye.com</a>
<b>Alan J. Laska</b>	(212) 808-7624	<a href="mailto:alaska@kelleydrye.com">alaska@kelleydrye.com</a>
<b>Pamela D. Kaplan</b>	(212) 808-7980	<a href="mailto:pkaplan@kelleydrye.com">pkaplan@kelleydrye.com</a>

Requirements – Employers must:	Self-Insured Plan		Fully Insured Plan	
	Do Not Use PHI	Use PHI	Do Not Use PHI	Use PHI
<b>Required Amendments</b> (if without valid authorization):				
Only use or disclose PHI as permitted by law.	N/A	X	N/A	X
Not use or disclose the PHI for employment-related actions or decisions, or in connection with any other benefit or employee benefit plan of the sponsor.	N/A	X	N/A	X
Ensure “adequate separation” of records and employees is established and maintained between the group health plan and the plan sponsor. Describe and restrict access to and use of PHI to the specific class of employees under the control of the plan sponsor that will be allowed access to the PHI disclosed by the group health plan (e.g., auditors, accountants and benefits personnel).	N/A	X	N/A	X
Report any improper use or disclosure of PHI to the group health plan. Include an effective mechanism for resolving issues of improper access or use of PHI by the identified employees or other individuals.	N/A	X	N/A	X
Allow individuals to inspect, obtain copies of, and amend PHI about themselves.	N/A	X	N/A	X
Provide individuals with an accounting of disclosures of PHI made within the six years prior to the request for such accounting.	N/A	X	N/A	X
Make its internal practices, books and records relating to the use and disclosure of PHI available to HHS for purposes of auditing the group health plan’s compliance with the rule.	N/A	X	N/A	X

Requirements – Employers must:	Self-Insured Plan		Fully Insured Plan	
	Do Not Use PHI	Use PHI	Do Not Use PHI	Use PHI
<ul style="list-style-type: none"> <li>■ Procedural Requirements:</li> </ul>				
Adopt clear, written privacy procedures and safeguards to protect PHI and track disclosures.	X	X	N/A	X
Distribute a “Notice of Privacy Policies” to participants to communicate its privacy policies and procedures.	X	X	N/A	X
Designate a privacy official.	X	X	N/A	X
Train employees so that they understand the privacy procedures.	X	X	N/A	X
Establish grievance procedures and sanctions for privacy rights violations.	X	X	N/A	X
Mitigate any known harmful effect resulting from a violation of its policies and procedures about which it has knowledge.	X	X	N/A	X
<b>Business Associate Requirements:</b>				
Negotiate or revise written contracts with “Business Associates” to incorporate specific language defining the responsibilities of each party to comply with HIPAA.	X	X	X	X
<b>Limited Procedural Requirements:</b>				
Not retaliate against employees who exercise their privacy rights.	X	X	X	X
Not require an individual to waive rights under the rule as a condition of providing treatment, receiving payment, enrolling in a health plan or being eligible for benefits.	X	X	X	X