

**BR** BROWN  
**BI** RUDNICK  
BERLACK  
ISRAELS<sup>LLP</sup>

Group Health Plan Compliance with **HIPAA** and **ERISA**:  
**NAVIGATING THE LEGAL AND  
ADMINISTRATIVE MAZE**

**Q & A**

**QUESTION AND ANSWER RESOURCE GUIDE**

**2003**

**Group Health Plan Compliance with HIPAA and ERISA:  
*Navigating the Legal and Administrative Maze***

**Table of Contents**

|   |    |
|---|----|
| I. Introduction   | 1  |
| II. Questions and Answers Relating to HIPAA   | 3  |
| III. Questions and Answers Relating to the New Claims Review Regulations  | 35 |
| IV. Questions and Answers Relating to Group Health Plan Document, Summary Plan Description and Document Disclosure Requirements | 49 |
| V. Conclusion and Practical Considerations  | 57 |
| VI. Glossary of Terms   | 59 |
| VII. Index  | 64 |

No question and answer contained in this Q&A Guide is intended to constitute legal advice by the Employee Benefits Practice Group at Brown Rudnick Berlack Israels LLP, and the Employee Benefits Practice Group expressly disclaims any such interpretation by any party. Rather, the Employee Benefits Practice Group intends that this Q&A Guide serve to assist employers in their dealings with their attorneys and other advisors regarding their legal obligations under HIPAA and ERISA.

## **GROUP HEALTH PLAN COMPLIANCE WITH HIPAA AND ERISA: NAVIGATING THE LEGAL AND ADMINISTRATIVE MAZE**

### **I. INTRODUCTION**

The Employee Benefits Practice Group at Brown Rudnick Berlack Israels LLP has produced this Q&A Guide for the benefit of employers seeking to obtain a basic understanding of the administrative challenges facing them (and there are many) as a result of the recent enactment of federal regulations in the area of Group Health Plan administration. Just in the past year, new and extremely complex claims review and privacy requirements have been imposed on employers sponsoring Group Health Plans. In addition, the United States Department of Labor (the “DOL”) has imposed substantial new requirements on employers for describing the terms and conditions of their Group Health Plans to their employees.

Complicating matters is the relative lack of coordination between the federal agencies responsible for ensuring compliance with the new rules. For instance, the DOL administers the new claims review and summary plan description content requirements, whereas the United States Department of Health and Human Services (“DHHS”) administers the new medical privacy rules. Each agency has issued regulations and other guidance for the areas within its purview, but neither agency has worked with the other to issue even minimally sufficient common guidance for areas in which the new rules overlap (especially regarding employer obligations in such situations).

Rarely has such a confluence of legal activity in the area of Group Health Plan administration occurred. It is the hope of the Employee Benefits Practice Group at Brown Rudnick Berlack Israels LLP that this Q&A Guide will serve as a valuable resource for employers seeking to navigate the “legal and administrative maze” created by the new requirements in a cost-effective manner.

The following discussion is presented in a question and answer format that is designed to educate, inform and assist employers in understanding the general requirements of the newly effective privacy rules enacted under the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”), and claims review and summary plan description content requirements enacted under the Employee Retirement Income Security Act of 1974, as amended (“ERISA”).

While the number and complexity of the legal requirements imposed upon employers may seem daunting, the Employee Benefits Practice Group at Brown Rudnick Berlack Israels has developed a comprehensive set of basic compliance materials that are available to employers at a reasonable fixed fee. In many cases an employer will be able to fulfill the vast majority of its legal obligations under HIPAA’s privacy rules and ERISA’s claims regulations through these

materials. Employers desiring additional information should contact any one of the attorneys in Brown Rudnick Berlack Israels LLP Employee Benefits Practice Group listed below:

|                            |              |                       |
|----------------------------|--------------|-----------------------|
| Harvey M. Katz             | 212-209-4860 | hkatz@brbilaw.com     |
| George L. Chimento         | 617-856-8503 | gchimento@brbilaw.com |
| James L. Hauser            | 617-856-8130 | jhauser@brbilaw.com   |
| Adam B. Cantor             | 212-209-4896 | acantor@brbilaw.com   |
| Pamela L. Kearse           | 617-856-8164 | pkearse@brbilaw.com   |
| Rita L. Gelman (Paralegal) | 212-209-4838 | rgelman@brbilaw.com   |

## II. QUESTIONS AND ANSWERS RELATING TO HIPAA

### A. Why do the HIPAA Privacy Rules matter to my company?

1. *Why should my company care about the HIPAA Privacy Rules?*

Any company that sponsors a “Group Health Plan” is likely to be affected by the HIPAA Privacy Rules in a variety of ways – as an employer, as a plan sponsor and, depending on the facts, as a plan administrator. The first step that any such company should take is ascertaining the extent to which it (or its group health plan) must comply with the HIPAA Privacy Rules (the “Privacy Rules”). If compliance with the Privacy Rules is necessary, the company should take steps to comply or modify its practices to minimize its compliance burden. (See question II.B.3. for a definition of the term Group Health Plan.)

2. *Don't the HIPAA Privacy Rules apply only to health plans and health care providers? In other words, aren't employers exempted?*

No. The HIPAA Privacy Rules apply to any “covered entity,” provided that certain other requirements are met. A covered entity (“Covered Entity”) means a health plan, health care clearinghouse or health care provider (to the extent that it engages in the electronic transmission of confidential health information). Because a Group Health Plan can be a Covered Entity, and the employer always serves as plan sponsor and frequently as plan administrator of its Group Health Plan, the HIPAA Privacy Rules can, and frequently do, apply to an employer.

3. *Under what circumstances will a Group Health Plan be a Covered Entity?*

A Group Health Plan will be a Covered Entity if it either (i) has 50 or more participants or (ii) is administered by a third party (e.g., an insurance carrier).

4. *Isn't my company's insurance carrier responsible for my Group Health Plan's compliance with the HIPAA Privacy Rules?*

No. Even if an insurance carrier handles the day-to-day administration of the plan, it is the employer's, and not the insurance carrier's, obligation to determine whether the HIPAA Privacy Rules apply to a particular set of facts. Such a determination generally requires a detailed and sophisticated review of the plan documents and the employer's practices and procedures regarding the overall administration of the plan. Most insurance carriers have not been trained to perform this analysis.

5. *If my company sponsors a fully insured Group Health Plan and does not handle confidential medical information on a day-to-day basis, does it need to comply with the HIPAA Privacy Rules?*

In most instances, yes. An employer that sponsors a fully insured Group Health Plan is still likely to need access to confidential medical information to:

- a) assist employees with claims payment and resolution of disputed claims;
- b) fulfill its fiduciary obligations under ERISA to monitor and supervise the compliance of its insurance carrier with the claims regulations issued by the DOL; and
- c) re-bid its Group Health Plan insurance coverage.

All of these issues are more fully discussed in Section II. C. of this booklet.

6. *What are the risks to my company of simply ignoring the HIPAA Privacy Rules?*

Any employer that violates the HIPAA Privacy Rules faces several risks. First, DHHS could audit the employer's (and the plan's) compliance with the Rules and fine the employer and its human resources employees for non-compliance. Second, employees whose rights have been violated could sue the employer (and the plan) under a state invasion of privacy law. Also, as a practical matter, the plan's health care providers and insurance carrier may refuse to provide confidential medical information to an employer that cannot demonstrate that it has complied with the requirements of the HIPAA Privacy Rules.

## **B. What are the general requirements of the HIPAA Privacy Rules?**

1. *What are the HIPAA Privacy Rules?*

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996, as amended. Lawmakers authorized DHHS to draft privacy regulations governing the use and disclosure of "protected health information," or PHI, by a Covered Entity essentially as a substitute for enacting a full-fledged "patient's bill of rights." The idea was to improve the security of patients' confidential health care information, but to do so in a way that promotes, or at least does not discourage, the electronic exchange of information among covered entities. These regulations and interpretative guidance published by DHHS comprise the HIPAA Privacy Rules (the "Privacy Rules").

2. *What is the basic intent of the Privacy Rules?*

The Privacy Rules provide guidelines for safeguarding the use and disclosure of certain confidential medical information known as PHI. The general requirement is that a

Covered Entity may not use or disclose PHI except as authorized by the individual who is the subject of the information or as explicitly required or permitted by the Privacy Rules. When the Covered Entity is the Group Health Plan, the Privacy Rules impose obligations on the employer in its roles as plan sponsor and plan administrator and prohibit the employer from using or disclosing PHI for improper employment purposes, such as when deciding to hire or fire an employee.

3. *What is a Group Health Plan?*

A Group Health Plan is a health plan that covers the employees of an employer and/or their beneficiaries (e.g., dependents and spouses covered under the plan) through (i) employer payments to health care providers, (ii) employer (and possibly employee) premium payments to an insurance carrier or HMO, (iii) employer reimbursement payments to covered individuals or (iv) any other means.

4. *What types of Group Health Plans are covered by the Privacy Rules?*

Almost all types of Group Health Plans are covered, including medical, dental, vision, prescription drug, health care flexible spending account plans and certain employee assistance programs, provided that they cover at least 50 participants or are administered by an entity other than the employer (e.g., the insurance carrier or HMO). Long-term disability, short-term disability, life insurance plans, stop loss and workers' compensation plans are not Group Health Plans under the Privacy Rules.

5. *What is PHI?*

PHI is "individually identifiable health information" that is transmitted or maintained electronically or in any other form or medium. "Individually identifiable health information", in turn, is information that (i) is created or received by a health care provider, health plan, employer, or health care clearinghouse, (ii) relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual and (iii) identifies the individual or creates a reasonable basis to believe that the information would identify the individual.

6. *What are some examples of PHI?*

Health information containing any of the following identifiers of the individual, or of relatives, employers or household members of the individual, would be considered PHI under the regulations: name, address, any date directly related to the individual (e.g., birth date, treatment date, discharge date), relatives' names, photographs, fingerprints, Social Security number, medical record number, health plan benefit number, telephone or fax number, account number, vehicle identification number or license plate number, e-

mail address, account numbers and any other individually identifying number, characteristic or code.

7. *Under what types of Group Health Plans is the typical employer likely to need access to PHI?*

The answer is primarily a fully insured or self-insured medical plan providing medical, dental, vision and/or prescription drug coverage. As a practical matter, the need for PHI is likely to be greatest with respect to the portion of the Group Health Plan providing medical benefits.

8. *If my company “de-identifies” the confidential medical information, does it have to comply with the Privacy Rules?*

The answer is no. Confidential medical information that is not “individually identifiable” is not PHI.

9. *What is “de-identified” confidential medical information?*

To be de-identified, health information must be stripped of all identifying data, or that information which would enable someone to recognize the individual who is the subject of the inquiry. The Privacy Rules contain a safe harbor that describes a series of specific items that must be deleted for the information to be de-identified, and it also allows for other statistically valid methods that are properly certified. The items that must be deleted under the safe harbor are the following:

- a) Names;
- b) All geographic subdivisions smaller than a state, except for the first three digits of a zip code, if the geographic unit formed by combining all of the zip codes with the same three initial digits contains more than 20,000 people (otherwise the first three digits must be changed to 000);
- c) All elements of dates (except year) for dates directly relating to an individual, including birth date, admission date, discharge date, date of death, all ages over 89, all indicators of age except when they may be aggregated into a single category of age 90 or older;
- d) Telephone numbers;
- e) Fax numbers;
- f) Electronic mail address;

- g) Social Security numbers;
- h) Medical record numbers;
- i) Health plan beneficiary numbers;
- j) Account numbers;
- k) Certificate/license numbers;
- l) Vehicle identifiers, including license plate numbers;
- m) Device identifiers;
- n) Web Universal Resource Locators (URLs);
- o) Internet Protocol (IP) address numbers;
- p) Biometric identifiers, including finger and voice prints;
- q) Full face photographic images and any comparable images; and
- r) Any other unique identifying number, characteristic or code.

**C. When do employers, plan sponsors and Group Health Plans become subject to HIPAA?**

1. *Is my company's medical plan subject to the HIPAA Privacy Rules?*

Yes, if your company's medical plan is a Group Health Plan that either covers at least 50 participants or is administered by a third party (i.e., is not "self-administered"). In addition, the plan must handle PHI.

2. *What are the most common types of Group Health Plans?*

Two types of Group Health Plans dominate the employer health care market: fully insured medical plans and self-insured medical plans. However, it is common for an employer to maintain other types of plans, such as dental plans, flexible spending accounts, employee assistance plans, and healthcare reimbursement accounts. The primary focus of this Q&A Guide is the portion of a Group Health Plan providing medical benefits.

3. *What is a “fully insured plan”?*

A “fully insured plan” is a Group Health Plan in which all payments for coverage are made by the insurance carrier or HMO providing benefits. The employer makes premium payments to the insurance carrier or HMO, which then pays the health care providers as covered medical costs are incurred. Other than making such premium payments, the employer does not incur any costs for making health care coverage available to its employees and/or the beneficiaries of its employees. In many instances, the employer requires its employees to make premium payments in partial payment of the coverage being provided.

4. *What is a “self-insured plan”?*

A “self-insured plan” is a Group Health Plan in which all payments for coverage are made by the employer from its general assets. To cap liability for high medical costs, an employer that “self-insures” almost always enters into a “stop loss” contract with an insurance carrier. Such a contract limits the employer’s out-of-pocket costs with respect to participant claims. It is common for both an individual and aggregate stop loss limit to apply.

5. *Is a “self-insured plan” that handles PHI subject to the HIPAA Privacy Rules?*

Many employers confuse the concepts of “self-insurance” and “self-administration”. A self-insured plan that is self-administered will be subject to the Privacy Rules if it (i) covers 50 or more participants and (ii) handles PHI. A self-insured plan that is not self-administered will be subject to the Privacy Rules if it handles PHI.

6. *Can a “fully insured plan” that covers fewer than 50 participants be subject to the HIPAA Privacy Rules?*

Yes. If the plan is not self-administered and handles PHI, it will be subject to the HIPAA Privacy Rules, even if it covers fewer than 50 participants. It should be noted, that for a fully insured plan, self-administration is quite rare. In most cases, such a plan is administered by the insurance carrier or HMO providing coverage.

7. *These rules seem complicated. Is there a simple way to keep track of them?*

Yes. Just refer to the chart below.

| Type of Plan              | Self-Administered   | Third Party Administration                   |
|---------------------------|---|--|
| <b>Self-Insured Plan</b>  | Subject to Privacy Rules if plan (i) covers at least 50 participants and (ii) handles PHI | Subject to Privacy Rules if plan handles PHI |
| <b>Fully Insured Plan</b> | Subject to Privacy Rules if plan (i) covers at least 50 participants and (ii) handles PHI | Subject to Privacy Rules if plan handles PHI |

8. *Under what circumstances is a Group Health Plan considered to be “self-administered”?*

In general, the answer to this question depends on whether the employer is involved in the day-to-day management of the plan. For a fully insured plan, self-administration is uncommon. Thus, in most cases, a fully insured plan is likely to be subject to the Privacy Rules, even if it covers fewer than 50 participants. For a self-insured plan, self-administration is a much more common arrangement.

9. *Does a Group Health Plan in which the employer serves as “plan administrator” always constitute a self-administered plan?*

No. If the employer serves as plan administrator only in name (e.g., due to legal requirements under ERISA), the plan generally will not constitute a self-administered plan. However, if the employer serves as plan administrator both in name and actual practice, the plan generally will constitute a self-administered plan. For instance, a fully insured plan in which the employer serves as plan administrator in name but contracts out the day-to-day management of the plan to the insurance carrier or HMO providing coverage almost certainly will not constitute a self-administered plan. Similarly, a self-insured plan in which the employer serves as plan administrator in name but contracts out the day-to-day management of the plan under an administrative services only, or “ASO”, contract, almost certainly will not constitute a self-administered plan.

10. *If the plan administrator of a plan that is not self-administered (i.e., is third party-administered) handles PHI on a day-to-day basis, is the plan subject to the Privacy Rules?*

Yes. The use or disclosure of PHI by a Group Health Plan administered by the insurance carrier or HMO that provides coverage makes the plan subject to the HIPAA Privacy Rules as a Covered Entity.

11. *If the plan administrator of a plan that is administered by an insurance carrier or HMO does not handle PHI on a day-to-day basis, is the plan subject to the Privacy Rules?*

Probably. There are two basic circumstances under which a plan administrator that does not handle PHI on a day-to-day basis would still need access to PHI. The first is to assist employees in resolving disputed claims and the second is to fulfill its fiduciary responsibilities to oversee ERISA's claims procedure requirements.

If the plan administrator assists employees and/or their beneficiaries with disputed claims, it will have to obtain access to PHI. In such a situation, the plan's handling of PHI, through the employer acting in its capacity as plan administrator, will make the plan subject to the Privacy Rules as a Covered Entity.

Even if the plan does not assist employees with disputed claims, it will most likely need to review PHI to ensure that the HMO or insurance carrier is fulfilling its responsibilities under ERISA's claims review procedures. Virtually all Group Health Plans under HIPAA are subject to ERISA's claims review procedures. Those procedures require the plan administrator to ensure that participants whose claims are denied are provided with detailed explanations and medical documentation for the denials. However, the ERISA regulations were recently finalized, and it is rare for an insurer or HMO to comply with the requirements of the regulations. If the plan administrator of a fully insured or self-insured plan does not review the information being provided by the insurer or HMO to participants whose claims are denied, it has not met its fiduciary obligations under ERISA.

12. *Can my company be subject to the Privacy Rules even if the Group Health Plan is not subject to such Rules?*

Yes. If your company is performing a plan sponsor function and handles PHI for such purpose. For instance, if your company handles PHI in connection with re-bidding insurance coverage for its Group Health Plan or amending or terminating its Plan, it will have compliance responsibilities under the Privacy Rules to satisfy.

13. *If my company sponsors a Group Health Plan covering at least 50 participants or being administered by an insurance company or HMO in which PHI is handled, is there any way to escape coverage under the Privacy Rules?*

Yes. Most of the requirements of the HIPAA Privacy Rules do not apply to an employer (or its Group Health Plan) if the plan is fully insured and the employer's use or disclosure of PHI is limited to (i) "summary health information" or (ii) participation, enrollment or dis-enrollment information.

14. *Does the same exemption apply to a self-insured plan?*

No. A self-insured plan that is not self-administered or that covers 50 or more participants must comply with all applicable requirements of the HIPAA Privacy Rules.

15. *What is “summary health information”?*

In general, “summary health information” is health information, which may be PHI, that (i) has been cleansed of most of its individually identifiable characteristics and (ii) in the aggregate, summarizes the claims history, claims expenses, or types of claims experienced by individuals covered under the employer’s Group Health Plan.

How does summary health information differ from “de-identified” health information?

As noted above, de-identified health information is not PHI, whereas summary health information may be PHI. What’s the difference?

The only difference between de-identified health information and summary health information is that summary health information can use a five-digit zip code. Given that summary health information may be PHI, a plan might be better off using de-identified information, if it can. As a practical matter, however, few plans can limit use or disclosure of confidential medical information to summary health information, let alone de-identified health information.

16. *What are the most common reasons for my company needing to have access to summary health information?*

Your company will need to access summary health information primarily for two purposes: (i) in the case of a fully insured plan, to re-bid insurance coverage for the plan; or (ii) in the case of a fully insured or self-insured plan, to make design changes to the plan.

17. *As a practical matter, will it be possible for my company to re-bid its insurance coverage if its access is limited to “summary health information”?*

Probably not. Most insurers will want to look at more detailed information, particularly if one or more individuals have recently suffered serious illnesses. Without specific information on these cases, the insurer is likely to assume that the serious illnesses will continue to generate large medical expenses and re-bid coverage on that basis. If your company wants to keep its medical plan costs to a minimum, it will most likely need to provide any prospective insurer with PHI.

18. *What is “participation, enrollment or dis-enrollment information”?*

In general, this is PHI that identifies an individual with respect to whether he or she is participating, has enrolled to participate or has ceased participating in the plan.

19. *What is the most common reason for my company needing to have access to participation, enrollment or dis-enrollment information?*

To enable it to process its payrolls, especially if employees are required to pay a portion of the insurance premiums to participate and such premiums are withheld by your company on a pre-tax basis.

20. *If a fully insured plan otherwise subject to the HIPAA Privacy Rules limits my company’s access to PHI to “summary health information” or “participation, enrollment or dis-enrollment information,” does the plan need to comply with the HIPAA Privacy Rules?*

If it truly were possible for your Group Health Plan to limit use or disclosure in this way, the answer generally would be no. Thus, your company would not have to ensure the Plan’s compliance with the most significant requirements of the Privacy Rules, such as (i) appointing a privacy officer, (ii) training employees in HIPAA compliance, (iii) establishing safeguards to protect the privacy of PHI, or (iv) amending the Plan to permit the use or disclosure of PHI. However, as a practical and legal matter, it is unlikely that even a fully insured plan would be able to eliminate its access to PHI.

21. *Why must a fully insured plan have access to PHI as a practical matter?*

In today’s competitive health care market, most insurers and HMOs use the claims process to control their costs. This leads to frequent disputes between the insurers and HMOs on the one hand and participants on the other. In most plans, the employer (acting as plan administrator) will need to be involved in the claims process to ensure that claims are processed in a fair and timely manner. Involvement in the claims process requires the employer to have access to PHI.

22. *Why must a fully insured plan have access to PHI as a legal matter?*

On January 1, 2003, compliance with revised DOL regulations governing claims denials became mandatory for all medical plans covered by ERISA. These regulations are described in Part III of this booklet. Among other things, the claims regulations require that the plan administrator provide extensive information to participants when a claim for benefits is denied. For example, if a claim for benefits is denied based upon a medical reason, the plan administrator must ensure that the decision is made by a medical professional and provide his or her name, a description of the medical reason for the denial, references to the plan provisions on which the denial is based, and an explanation of how the plan provisions apply to the participant’s medical condition. In a

fully insured plan, the claims processing function is almost always delegated to the insurer or HMO by the plan administrator. However, the plan administrator has a fiduciary obligation to supervise the insurer or HMO, essentially to monitor such entity's compliance with these requirements. The plan administrator must have access to PHI in order to perform this necessary fiduciary function.

*23. Is my company subject to the Privacy Rules when acting in its employer (as opposed to its plan administrator or plan sponsor) capacity?*

An employer that sponsors a Group Health Plan may wear up to three hats: an employer hat, a plan sponsor hat and a plan administrator hat. The Privacy Rules apply to an employer (albeit indirectly) only when it is wearing its plan sponsor or plan administrator hat. When an employer acts as plan administrator, the Plan itself is the Covered Entity, but the employer, acting on behalf of the Plan, has HIPAA compliance responsibilities. When an employer acts as plan sponsor (e.g., when it re-bids insurance coverage), it may receive PHI as an employer (rather than as a plan administrator), but it is subject to the Privacy Rules because the information is being used for a Plan purpose. When an employer receives confidential information for an employment purpose pursuant to an authorization (e.g. to implement a sick leave program), the information it receives is not PHI because it is not being used for a Plan purpose. However, if the information is not obtained pursuant to a written authorization, it continues to be PHI and the employer will have violated the Privacy Rules.

*24. Under what circumstances will my company be considered to be wearing its "plan administrator" hat for purposes of the Privacy Rules?*

If your company designates itself as plan administrator under its Group Health Plan, it wears its plan administrator ("Plan Administrator") hat when it performs a Plan Administrator function, such as assisting with disputed medical claims. As required under ERISA, if your company has not made a formal designation of any person or entity as Plan Administrator, it must serve as the "default" Plan Administrator. The employer is the plan administrator in the vast majority of employer-sponsored medical plans.

*25. Under what circumstances will my company be considered to be wearing its "plan sponsor" hat for purposes of the Privacy Rules?*

When the employer is accessing PHI while performing a plan sponsor ("Plan Sponsor") function, such as adopting, amending or terminating the Group Health Plan or re-bidding insurance coverage under the plan.

26. *Under what circumstances will my company be considered to be wearing its “employer hat”?*

Generally, two situations exist in which your company might need to access PHI while wearing its employer hat. First, your company may be required to use or disclose PHI pursuant to another federal or state employment-related law, such as the federal Family and Medical Leave Act (“FMLA”) or the federal Americans with Disabilities Act (“ADA”). Second, your company may need to access PHI in order to administer a company-provided disability, sick leave, employee assistance or similar program.

27. *What are the consequences of my company wearing its employer hat with respect to PHI?*

The answer depends on whether your company obtains the PHI pursuant to a signed authorization by the participant or beneficiary. Assuming that this occurs, the confidential medical information ceases to constitute PHI (and instead becomes an employment record) and, therefore, the plan ceases to be subject to the Privacy Rules with respect to such information. In the absence of a signed authorization, the confidential information continues to constitute PHI and the plan continues to be subject to the HIPAA Rules with respect to such information. Given the latter possibility, your company should consider, each time that it creates, receives, or uses a piece of confidential health information about an employee, whether it is creating, receiving, or using the health information in its capacity as an employer or in its capacity as Plan Sponsor or Plan Administrator.

28. *Are there any federal or state laws that seem like employment-related laws but which nonetheless impose Privacy Rules compliance obligations on the plan?*

Yes. The quintessential example is a state workers’ compensation law. If the workers’ compensation law requires disclosure of PHI to the employer or if such disclosure is authorized pursuant to a signed authorization of the employee, the information continues to be PHI, but the Plan may disclose it to the employer without regard to the “minimum necessary standard.” If, however, the workers’ compensation law merely permits such disclosure, the “minimum necessary” standard will apply, unless the employee gives the plan a signed authorization for such disclosure.

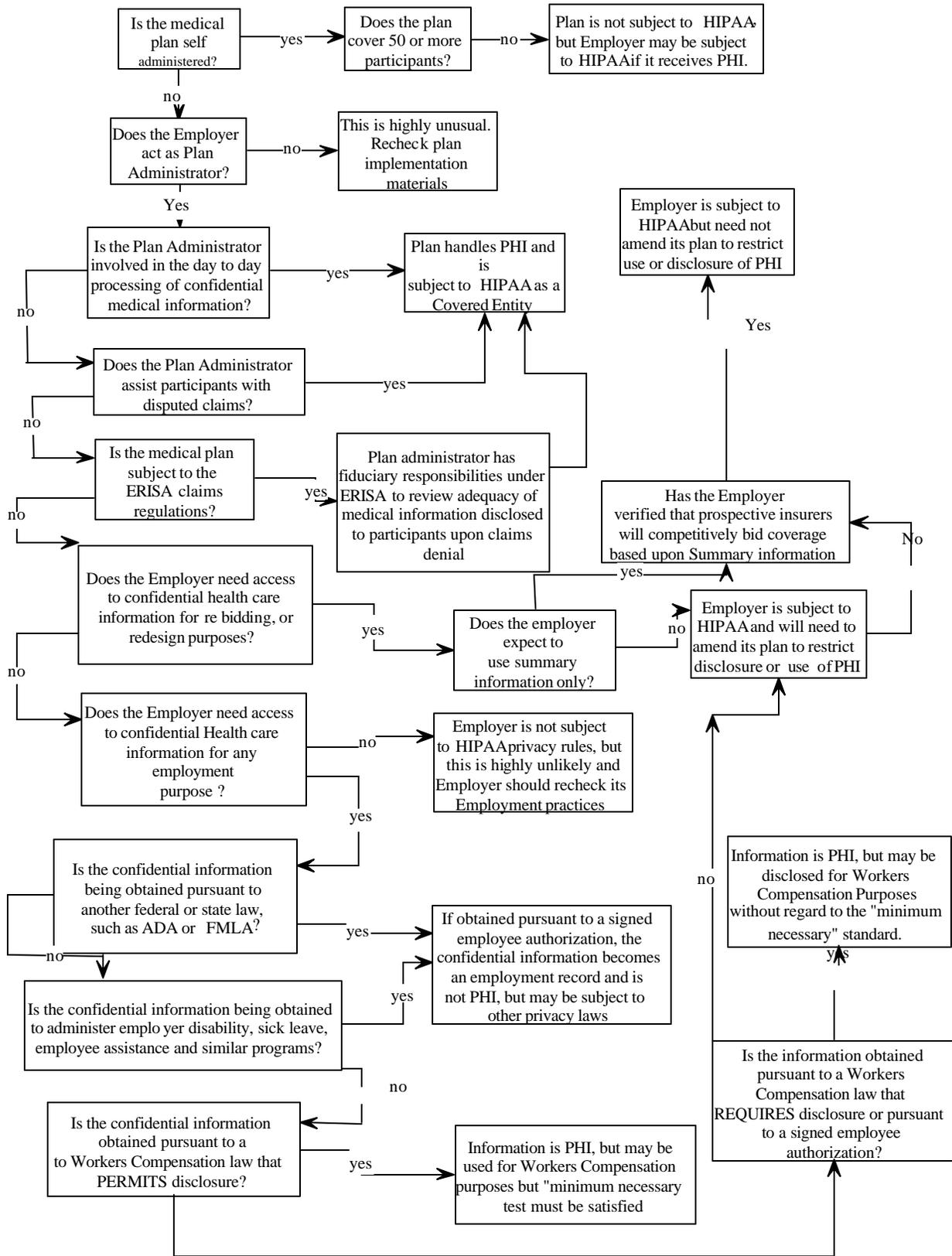
29. *What is the “minimum necessary” standard?*

Basically, the “minimum necessary” standard requires the Covered Entity to limit disclosure of PHI to the minimum information necessary to satisfy the inquiry. For example, if PHI is disclosed to the employer to enable it to administer a workers’ compensation program that permits, but does not require, such disclosure, the Group Health Plan cannot simply hand over the employee’s entire medical file. It must limit

disclosure to matters relevant to the workers' compensation inquiry. Where PHI is requested by a state workers' compensation official or other public official for a workers' compensation purpose, the Plan is permitted reasonably to rely on the official's representations that the information requested is the minimum necessary for the intended purpose.

30. *The HIPAA Privacy Rules affect my company in a variety of ways, depending on whether my company's Group Health Plan is self-administered, third-party administered, self-insured or fully insured and whether my company is wearing its employer, Plan Sponsor or Plan Administrator hat. How can my company keep track of such complex rules?*

It is not easy. However, reviewing the flowchart that appears below is a good starting point. In addition, it would be prudent for your company to retain legal counsel to assist it in identifying and then complying with its obligations under the Privacy Rules.



#### **D. What requirements do the HIPAA Privacy Rules impose on an employer that handles PHI?**

1. *What general rules apply to my company's use or disclosure of PHI in its capacity as Plan Administrator?*

Your company, acting as Plan Administrator of its Group Health Plan, may use or disclose PHI only with the authorization of the individual who is the subject of the PHI or as explicitly permitted or required by HIPAA.

The basic principles of the HIPAA Privacy Rules are straightforward: A Covered Entity (e.g., your Group Health Plan, through your company as Plan Administrator) may not use or disclose PHI, except in the following limited circumstances:

- a) disclosure to the individual;
- b) use or disclosure (for which the participant's consent may, but need not be, required) in order to carry out treatment, payment or health care operations, unless such use or disclosure relates to psychotherapy notes or marketing purposes;
- c) if not for treatment, payment or health care operations, use or disclosure pursuant to a signed, dated and narrowly crafted authorization; or
- d) disclosure to the government (state or federal) for purposes of public health, abuse/neglect investigation, fraud prevention, etc.

The Privacy Rules require a Group Health Plan and, therefore, the employer serving as Plan Administrator with respect to it, to:

- a) absent special authorization, use and disclose PHI only for activities permitted under the Privacy Rules – chiefly activities related to treatment, payment or health care operations;
- b) describe in a written notice distributed to Plan participants, the uses and disclosures it makes of PHI, unless the Plan is fully insured and the Plan Sponsor creates or receives only summary health information or participation, enrollment, or disenrollment information;
- c) enter into contracts with other entities that create or receive PHI in the course of providing services to the plan (e.g., enrollments, changes, or terminations of healthcare coverage) that require the other entities ("Business Associates") to use and disclose the PHI consistent with the Privacy Rules and, among other things, to make the PHI available to participants for copying and amendment;

- d) implement policies and procedures allowing participants to access and copy their PHI, request restrictions on its use, request amendments to it and request an accounting of certain types of PHI disclosures; and
- e) develop policies restricting employee access to the PHI of others, protecting PHI with physical, technical and administrative safeguards, and limiting the type of data transmitted or received to that which is minimally necessary for the function being performed.

2. *What is meant by “treatment, payment or health care operations”?*

The term “treatment” generally refers to the provision, coordination and management of health care. The term “payment” generally refers to tasks such as eligibility or coverage determinations, claims review, utilization review, coordination of benefits and medical necessity determinations. The term “health care operations” generally refers to certain services or activities necessary to carry out the covered functions of the health plan, such as business planning and development, underwriting and premium rating review, auditing claims for plan benefits and the exchange of PHI in connection with certain business transactions.

3. *Given that “payment” can include claims review-related activities, does my company, in its capacity as Plan Administrator, need participant consent or authorization to access a participant’s PHI when it assists such participant with a denied claim?*

The answer is that it depends. If the claim denial relates solely to a denial of payment for a previously performed medical procedure, neither consent nor authorization is required. However, as a practical matter, your company, acting as Plan Administrator of its Group Health Plan, may not wish to get involved in assisting a participant with a denied claim for payment unless the participant gives his or her consent or authorization. As noted in question 5 below, HIPAA does not preempt state privacy rules that provide greater rights to participants. If the claim relates to a request for urgent care or for care in the future, the “payment” exception to consent or authorization does not apply.

4. *What is a Business Associate?*

The Privacy Rules require Group Health Plans to enter into special agreements with service providers that come into contact with PHI. The Rules recognize that Group Health Plans will need to disclose PHI on a regular basis to their service providers, yet many of those service providers are not covered entities. Accordingly, the Privacy Rules require service providers to agree to treat PHI in a way which is similar to the way in which the Group Health Plan must treat it.

A service provider must enter into such an agreement before a Group Health Plan may disclose PHI to it. The agreement must require the service provider to comply with a number of standards, including, but not limited to, the following:

- a) using or disclosing PHI only as permitted under the agreement or as required by law;
- b) establishing appropriate safeguards to prevent impermissible use or disclosure of PHI;
- c) reporting known misuse of PHI by the service provider to the Plan;
- d) imposing the same requirements on its subcontractors and agents; and
- e) making an accounting of uses and disclosures of PHI available to participants in the Plan.

The term used by the Privacy Rules for an entity that uses or discloses PHI on behalf of a covered entity (such as a Group Health Plan) is Business Associate.

The term is defined as a person who, on behalf of a Covered Entity, performs (or assists in the performance of) a function or activity involving the use or disclosure of PHI.

Examples of such functions or activities given in the Privacy Rules include: claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing, or any other function or activity regulated by the Privacy Rules.

In addition, the Privacy Rules specifically identify the following services which, if they involve PHI, will make that person or entity a Business Associate:

- Legal
- Administrative
- Management
- Accounting
- Actuarial
- Accreditation
- Data aggregation
- Consulting
- Financial

A business associate cannot be an employee of a Covered Entity.

5. *If my company is subject to the Privacy Rules, does it still need to comply with state privacy laws?*

Possibly. The Privacy Rules do not preempt all state privacy laws. State privacy laws that are "more stringent" are preserved. That is, any state privacy law that provides more privacy protections or greater individual rights than provided by the federal Privacy

Rules will apply, unless that law is otherwise preempted by a different federal law, such as ERISA. Generally, state laws that are preempted by ERISA will remain preempted.

6. *Does my company need to comply with other federal laws that require it to use or release PHI?*

Generally, nothing in the Privacy Rules exempts an employer from having to comply with other federal laws (e.g., ERISA, ADA, FMLA).

7. *What is the timeline for compliance with the Privacy Rules?*

The implementation deadline is April 14, 2003, except for “small Group Health Plans,” which have until April 14, 2004. A small Group Health Plan is one with less than \$5,000,000 in gross annual receipts.

8. *What are my company’s “use or disclosure” obligations when it receives PHI in its capacity as Plan Sponsor or Plan Administrator of its Group Health Plan?*

If your company decides that it needs to receive PHI from its Group Health Plan (a Covered Entity) to fulfill its Plan Sponsor or Plan Administrator duties, it must ensure that the Plan documents are amended to:

- a) incorporate provisions to establish the permissible and required uses and disclosures that the Plan Sponsor or Plan Administrator may make; and
- b) provide that the Group Health Plan will only disclose information to the Plan Sponsor or Plan Administrator upon receipt of the Plan Sponsor’s or Plan Administrator’s certification that the Plan documents have been amended and that the Plan Sponsor or Plan Administrator agrees to:
  - (1) use and disclose PHI only to the extent permitted or required by the Plan documents;
  - (2) ensure that any of its agents who view PHI agree to the same conditions and restrictions that govern the Plan Sponsor’s or Plan Administrator’s use and disclosure of information;
  - (3) refrain from using or disclosing the information for employment-related actions and decisions in connection with another benefit or employee benefit plan of the Plan Sponsor;
  - (4) report any unauthorized use or disclosure of which it becomes aware;
  - (5) allow individuals access to their PHI as required;

- (6) allow amendments to PHI as required by the Privacy Rules;
- (7) make information available to provide for an accounting of disclosures as required by the Privacy Rules;
- (8) make its internal practices, books and records relating to the use or disclosure of PHI received from the Group Health Plan available to the Secretary of DHHS for purposes of determining compliance with the Privacy Rules;
- (9) to the extent feasible, return or destroy all PHI received from the Group Health Plan which is no longer needed; and
- (10) ensure that an adequate “fire wall” between the Plan and the Plan Sponsor/Plan Administrator exists, describing which employees have access to the PHI, restricting access to such individuals and for such use as is necessary for Plan administration functions, and providing methods by which noncompliance can be resolved.

The certification described above does not relieve your company, in its capacity as Plan Sponsor/Plan Administrator, from actually complying with these requirements.

9. *What constitutes an adequate “fire wall” for purposes of the Privacy Rules?*

No hard and fast rules exist, beyond the need to amend the Plan documents in the manner described above. The key is that your company must ensure that PHI needed for valid Plan Sponsor and/or Plan Administrator purposes is maintained separately from other PHI that the Plan handles.

10. *May a Group Health Plan disclose PHI to a Plan Sponsor or Plan Administrator if the requirements specified in question 8 have not been met?*

To a Plan Administrator, no. To a Plan Sponsor, only if the information being disclosed is summary health information that will be used to re-bid insurance coverage and/or amend or terminate the Plan.

11. *Are there any other “use or disclosure” obligations that apply to the Plan and, by extension, to my company as Plan Administrator?*

Yes. The Plan generally must comply with the minimum necessary standard.

12. *What must the Plan Administrator of a Group Health Plan do to ensure that the minimum necessary standard is met for each use and disclosure of PHI?*

In order to ensure that the minimum necessary standard is met, the Privacy Rules require the Plan Administrator of a Group Health Plan to do the following:

- a) identify those members of the Plan's (insurance carrier's, in the case of a Plan that is not self-administered; otherwise, the employer's) workforce who need access to PHI to carry out their duties. For each of those persons, the categories of PHI needed should be identified; and
- b) make reasonable efforts to limit the access of the Plan's workforce consistent with those determinations.

For routine and recurring disclosures, whether they are requests from other Covered Entities to the Group Health Plan or from the Group Health Plan to other Covered Entities, the Group Health Plan must draft and implement policies and procedures limiting the PHI disclosed or requested to the minimum necessary.

For non-routine disclosures, whether they are requests from other Covered Entities to the Group Health Plan or from the Group Health Plan to other Covered Entities, the Group Health Plan must develop criteria designed to limit the disclosure to the minimum necessary. It must review individual disclosures to ensure the minimum necessary standards are met.

13. *What are the administrative obligations of my company if it handles PHI?*

An employer that handles PHI has many obligations. Not only must such an employer comply with the rules governing use and disclosure, but it also must comply with a litany of administrative requirements, including, but not limited to, the following:

- a) designating a privacy official;
- b) designating a contact person responsible for receiving complaints;
- c) training human resources employees on the policies and procedures;
- d) establishing appropriate administrative, technical and physical safeguards to protect the privacy of PHI;
- e) providing a process for individuals to make complaints;
- f) applying appropriate sanctions against members of its workforce who fail to comply;

- g) mitigating harmful effects of violations of policies and procedures;
- h) refraining from engaging in intimidating or retaliatory acts against individuals who exercise their rights under the Privacy Rules;
- i) maintaining compliance logs for six years of all employee complaints, requests for restrictions on the use or disclosure of PHI and accountings of disclosure of PHI (certain exceptions apply); and
- j) establishing policies and procedure to comply with the Privacy Rules.

14. *What is the function of the privacy official?*

The privacy official serves as the individual responsible for coordinating your company's HIPAA compliance efforts – i.e., ensuring that all of the other tasks described in question 13 above are undertaken in compliance with the Privacy Rules.

15. *What kind of training must my company give its employees to comply with the Privacy Rules?*

The Privacy Rules require that an employer train all employees on its policies and procedures with respect to PHI, as necessary for them to carry out their functions. As a practical matter, however, this means training the human resources employees to whom access to PHI is being granted in the basic prohibitions of the Privacy Rules and the employer's policies and procedures regarding the use or disclosure of PHI. Training must be done within a reasonable period of time after the date of hire and, for each employee whose functions are affected by a material change in the employer's policies and procedures, within a reasonable time after the change becomes effective.

16. *What would be examples of intimidating or retaliatory acts prohibited by the Privacy Rules?*

Clearly, firing an employee or refusing to promote or increase the compensation of an otherwise eligible employee who has exercised his or her rights under the Privacy Rules would be prohibited. In any event, whether an act is intimidating or retaliatory will generally depend on the particular facts and circumstances.

17. *Is my company required to ensure that the Plan's service providers protect PHI?*

Yes. The Privacy Rules are designed to ensure that entities helping to administer the Group Health Plan protect the PHI of participants and beneficiaries to the same extent that the Group Health Plan is required to do so.

At the first level, the Privacy Rules require employers to safeguard the PHI they have received from the Group Health Plan and to use or disclose it only as permitted in the Plan documents. The employer is also required to include similar protections in any contract it enters into for purposes of Plan administration.

At the second level, the Privacy Rules require Covered Entities, including Group Health Plans, that contract with service providers to enter into contracts under which the service providers agree to safeguard PHI received or created in the course of the business relationship. These contracts are called "Business Associate Contracts." Business Associates are also required to include similar protections in any contracts they enter into for purposes of providing services to the Covered Entities (that is, subcontracts must include similar requirements).

Traditionally, Plan Sponsors or Plan Administrators (not the Group Health Plans) enter into service provider contracts for purposes of administering the Plans. While Plan Sponsors and Plan Administrators are not Covered Entities or Business Associates, their contracts with service providers are required to have business associate-like language.

18. *What happens if the Group Health Plan makes an accidental disclosure relating to permissible uses and disclosures?*

The Privacy Rules allow "incidental disclosures" by Group Health Plans and other Covered Entities. Incidental disclosures are ones that occur as by-products of a use or disclosure permitted under the Rules. While this exception was drafted with health care providers in mind, it also applies to Group Health Plans.

An incidental disclosure will not be a violation of the Privacy Rules if:

- a) it occurs as a by-product of a permitted use or disclosure;
- b) only the minimum necessary PHI was used or disclosed; and
- c) appropriate safeguards were in place to prevent such a disclosure.

**E. What are my company's obligations to its Group Health Plan participants under the Privacy Rules?**

1. *What rights do my company's Group Health Plan participants have with respect to their PHI?*

To emphasize the impact of the Privacy Rules on your company, it is essential to review some of the protections afforded to Group Health Plan participants and beneficiaries by the Rules. Included among the rights granted to Group Health Plan participants and beneficiaries under the Privacy Rules are the following rights:

- a) To receive notice of the Group Health Plan's privacy practices

Because a Group Health Plan is a Covered Entity, employees and beneficiaries participating in the Plan must receive information about the Plan's procedures to ensure the privacy of their health care information. Among other items, the notice must include examples of PHI disclosures that do not require a participant's or beneficiary's authorization and examples of those that do, a statement that the Group Health Plan is required by law to maintain the privacy of PHI, a statement of the individual's rights with respect to his or her PHI and how these rights can be exercised, and information as to how an individual can complain if he or she believes that his or her rights have been violated.

- b) To request that disclosures of their PHI be restricted, for example, to only certain individuals or only to carry out treatment, payment or health care operations

However, the Group Health Plan is not obligated to grant a request that is unreasonable or too burdensome.

- c) To request that alternative methods be used to release their PHI

The Group Health Plan must comply if the PHI is readily producible in the form or format being requested.

- d) To inspect and obtain a copy of their PHI

This is one of the broadest rights provided by the Privacy Rules, and exceptions are very limited. A Group Health Plan must comply with a participant's or beneficiary's request within 30 days; if it does not, it must explain its reasons for not doing so. This right may extend to PHI received and stored by employers.

- e) To request amendments to their PHI

While a Group Health Plan may deny this request if the PHI is "accurate and complete" or if the Plan did not actually create the PHI, if it grants the request, it must inform both the participant or beneficiary and all others who may need to know of the change, such as other health care providers.

- f) To receive information about the disclosures of their PHI

Participants and beneficiaries can request details of all disclosures of their PHI going back six years. However, this list of disclosures does not have to include releases needed to carry out treatment, payment, and healthcare operations—i.e., the primary permitted uses of PHI under the Privacy Rules.

2. *When must the Group Health Plan provide the notice of privacy rights?*

To new enrollees, at the time of enrollment. Also, if the notice is materially revised, within 60 days of the date of such revision(s), to individuals then covered by the Plan.

3. *What is the difference between “consent” and “authorization” under the Privacy Rules?*

The Privacy Rules permit, but do not require, a Covered Entity voluntarily to obtain participant or beneficiary consent for uses and disclosures of PHI for treatment, payment, or health care operations. Covered Entities that do so have complete discretion to design a process that best suits their needs.

By contrast, the Privacy Rules require an “authorization” for uses and disclosures of PHI that are not otherwise allowed by the Rules. Where the Privacy Rules require participant or beneficiary authorization, voluntary consent is not sufficient to permit a use or disclosure of PHI unless it also satisfies the requirements of a valid authorization. An authorization is a detailed document that gives a Covered Entity permission to use PHI for specified purposes, which are generally purposes other than managing treatment, payment, or health care operations, or to disclose PHI to a third party specified by the individual. An authorization must contain a number of elements, including, but not limited to, a description of the PHI to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the Covered Entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed. With limited exceptions, a Group Health Plan may not condition treatment or coverage on the individual providing an authorization.

The Privacy Rules distinguish between consent and authorization very specifically:

- a) A participant’s or beneficiary’s consent is now optional when PHI is needed to carry out treatment, payment, or health care operations. Under the Privacy Rules, the amount of information that can be disclosed related to treatment, payment, or health care operations is limited to just what is necessary and not everything that is available on a particular participant.
- b) A participant’s or beneficiary’s authorization must be obtained if the PHI is to be used for any purpose other than treatment, payment, or health care operations. The Group Health Plan has to make it clear that it is not requiring such authorization before it allows treatment, payment, enrollment in the health plan, or eligibility for benefits, except in some specific situations, such as a research project; enrollment or eligibility prior to the individual’s enrollment in a health plan; and payment of health claims if this disclosure is necessary—but such disclosures cannot include psychotherapy notes.

- c) Marketing is one major area where authorization will be required. The Privacy Rules clearly prohibit Group Health Plans from selling personal medical information to a business that wants to market its products and services under a business associate agreement.
- d) The release of psychotherapy notes also requires the participant's or beneficiary's specific authorization, even as part of normal treatment and business operations. In other words, psychotherapy notes are not covered the way other PHI is handled under "treatment, payment, and business operations," the more restrictive authorization is required for the release of this information for these purposes. However, psychotherapy notes do not, for example, include medical records of mental health diagnoses. Psychotherapy notes mean only "notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session and that are separated from the rest of the individual's medical record."

(1) Some exceptions apply, including the release of psychotherapy notes for treatment by the person who created the notes; to conduct training; and to defend legal action brought by the participant or beneficiary. Authorization is also not needed when psychotherapy notes are required for law enforcement purposes; when mandated by law; when needed for supervision of the provider who created the notes; when required by a coroner or medical examiner; or when needed to counter a major threat to health or safety.

4. *When may my company's Group Health Plan disclose health information to the personal representative of a participant or beneficiary?*

Generally, your company's Group Health Plan may disclose health information to the personal representative of a participant or beneficiary, and should treat the personal representative the same as the participant or beneficiary (but only with respect to PHI relevant to such personal representative).

There are two major exceptions to this rule:

- a) Certain disclosures to parents or guardians of unemancipated minors.
- b) In situations where the Group Health Plan believes that it is not in the best interests of the participant or beneficiary to treat someone as his or her personal representative because:

(1) the Group Health Plan reasonably believes the participant or beneficiary has been or may be abused or neglected by the personal representative; or

(2) the Group Health Plan reasonably believes that the participant or beneficiary will be endangered if the personal representative is treated as such.

5. *When may my company's Group Health Plan disclose PHI to the personal representative of an unemancipated minor?*

The Privacy Rules defer to state law with respect to the access of parents and guardians to the protected health information of unemancipated minors. If state law explicitly requires, permits, or prohibits disclosure of PHI to a parent, then that state law applies. Similarly, state law applies to the parent's or guardian's ability to assert the unemancipated minor's right of access.

6. *When may my company's Group Health Plan disclose health information about a deceased individual?*

Generally, the Privacy Rules require that a Group Health Plan protect deceased individuals' PHI in exactly the same way that it would protect living individuals' information. If, however, under applicable law, an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, the Group Health Plan must treat that person as a personal representative of the deceased. Personal representatives of the individual are to be treated as though they are the individual.

7. *What kinds of restrictions on use or disclosure of PHI can a participant or beneficiary request?*

Participants and beneficiaries can request restrictions on only two categories of a Group Health Plan's uses and disclosures of PHI:

- a) uses and disclosures made for treatment, payment or health care operations; and
- b) disclosures made to family members or other individuals directly involved in the participant's or beneficiary's care.

Participants and beneficiaries have no right to request Group Health Plans to restrict other uses and disclosures permitted under the Privacy Rules. A Group Health Plan could agree to restrict other uses and disclosures, but those restrictions are not enforceable under the Privacy Rules.

8. *What is the right to request confidential communications?*

Participants and beneficiaries can request that a Group Health Plan provide communications of PHI by alternative means or at alternative locations, if the participant or beneficiary states that the disclosure of the information could endanger him or her.

- a) Example of "alternative location": A participant or beneficiary who does not want his family members to know about a certain treatment may request the Group Health Plan to communicate with him at his place of employment, by mail to a designated address, or by phone to a designated phone number.
- b) Example of "alternative means": A participant or beneficiary may request the Group Health Plan to send communications in a closed envelope rather than a post card.

9. *What information does a Group Health Plan have to make available?*

A Group Health Plan generally must permit a participant or beneficiary to inspect and get a copy of certain PHI in a Group Health Plan's "designated record sets."

A Group Health Plan's "designated record sets" include the following:

- a) the enrollment, payment, claims adjudication, and case or medical management records systems maintained by or for the Group Health Plan.
- b) all other records used, in whole or in part, by the Group Health Plan to make decisions about participants and beneficiaries.

If the information is in the Group Health Plan's designated record sets, the Group Health Plan must grant access, even if it did not create the information, unless it is able to assert one of the grounds for denial of access specified in the Privacy Rules.

Also, if the information is in the Group Health Plan's designated record sets, the Group Health Plan must grant access even if the information was obtained or created before the effective date of the Privacy Rules.

A Plan does not have to grant access to all information contained in its designated record sets. For example, if a designated record set includes PHI in quality control records, and those records are not used to make decisions about the participants or beneficiaries requesting access, then those records are not (and should not be) disclosed to the participants or beneficiaries requesting access.

10. *What is the “right to request an amendment”?*

Participants and beneficiaries have the right to request that their Group Health Plan amend their PHI if they believe that information is inaccurate or incomplete. The purpose of this right is to give participants and beneficiaries a way to ensure that information about them is as accurate as possible as it travels through the health care system and is used to make decisions about them. Participants and beneficiaries do not have a right to actually have their records changed, however. The right is only to request the change.

Under the Privacy Rules, when a Group Health Plan “amends” a record, it may either append the change to an existing record or create a new record. Note that some state laws may prohibit information in medical records from being changed or deleted. Your company may want to analyze whether, under the ERISA and HIPAA preemption rules, those laws apply to its Group Health Plan’s medical records containing PHI.

11. *Who has the right to request an amendment of PHI?*

A participant or beneficiary, or the participant's or beneficiary's personal representative, has a right to request amendment of the participant's or beneficiary's PHI.

12. *How long may a Group Health Plan take to decide whether to grant or deny a request for amendment?*

A Group Health Plan must act on an individual's request for amendment within 60 days after receiving the request as follows:

- a) Denial of Requests. If the Group Health Plan denies the request for amendment, a written denial must be sent to the participant or beneficiary within this 60-day time frame.
- b) Grant of Requests. If the Group Health Plan grants the request for amendment, it must make the amendment and notify the individual that it has done so within this 60-day time frame.

13. *Can my company, in its role as Plan Sponsor of its Group Health Plan, condition participation in such Plan upon the participant's or beneficiary's agreement to sign an authorization form?*

An employer sponsoring a Group Health Plan generally is prohibited from conditioning enrollment in the Plan, or payment of benefits under the Plan, on an authorization. The exceptions that exist for this prohibition for other types of health plans generally do not apply to Group Health Plans. For instance, while health plans can condition enrollment on obtaining an authorization for the release of PHI for underwriting or risk rating

purposes, this exception best applies to health plans offering individual underwritten policies.

Although a Group Health Plan cannot condition enrollment in the plan on the signing of an authorization, employers (who are not Covered Entities) appear to be able to condition employment on an authorization.

## **F. How are the HIPAA Privacy Rules enforced?**

### *1. What are the penalties for non-compliance?*

HIPAA imposes civil and criminal penalties for failing to comply with the Privacy Rules. Penalties begin at \$100 per violation, up to a maximum of \$25,000.

Criminal penalties apply for a deliberate offense, as an intent to sell PHI, ranging from \$50,000 and one year in prison up to \$250,000 and ten years.

HIPAA also makes an employer liable for violations of its Business Associates if the employer is aware of the wrongdoing.

### *2. What federal agencies are responsible for enforcing HIPAA's Privacy Rules?*

DHHS is responsible for enforcing civil penalties under HIPAA. For purposes of the Privacy Rules, the Secretary of DHHS has delegated this authority to the agency's Office for Civil Rights ("OCR"). For purposes of the other HIPAA Rules (e.g., Electronic Transactions, Security), the Secretary has delegated this authority to the Centers for Medicare & Medicaid Services ("CMS"). The U.S. Department of Justice ("DOJ") will enforce the criminal penalties.

### *3. How do individuals who believe they have been harmed by improper use or disclosure of their PHI sue?*

HIPAA does not give the individual a "private right to action." The individual may have a tort claim under state law or pursuant to legal rights established outside of HIPAA, and may retain legal counsel to enforce such a claim if he or she believes that he or she has been harmed. However, HIPAA does provide a right to file complaints or grievances with DHHS or with a covered entity's "privacy official." DHHS will then, in its discretion, review complaints, launch investigations, pursue civil remedies or refer matters to DOJ to prosecute alleged criminal acts -- as it sees fit. DHHS and DOJ have the authority to bring HIPAA lawsuits, but individuals do not.

## **G. How do the Privacy Rules apply to employee benefit plans that are not health plans?**

1. *Are the following types of insurance covered under HIPAA: long/short term disability; workers' compensation; and automobile liability that includes coverage for medical payments?*

No, the listed types of policies are not health plans. The Privacy Rules specifically exclude from the definition of a "health plan" any policy, plan, or program to the extent that it provides, or pays for the cost of:

- a) coverage only for accident, or disability income insurance, or any combination thereof;
- b) coverage issued as a supplement to liability insurance;
- c) liability insurance, including general liability insurance and automobile liability insurance;
- d) workers' compensation or similar insurance;
- e) automobile medical payment insurance;
- f) credit-only insurance;
- g) coverage for on-site medical clinics; and
- h) other similar insurance coverage, specified in regulations, under which benefits for medical care are secondary or incidental to other insurance benefits.

Therefore any information obtained by the employer in connection with these programs is not PHI (except information necessary to comply with mandatory requirements of workers' compensation or similar law). As noted above, the Privacy Rules apply only when PHI is involved.

2. *How do the Privacy Rules interact with Federal employment laws and other employment-related arrangements?*

- a) Americans with Disabilities Act ("ADA")

Employers often require medical information to determine whether an employee has a protected disability and whether an employee can safely and effectively perform the essential functions of his or her job. DHHS made clear in the August 2002 modifications to the final Privacy Rules that this is an employer function, which does not implicate the Privacy Rules. In this instance, the employee will need to see a physician or other health care provider in order to obtain the necessary certification.

Since the provider is likely to be a Covered Entity that is subject to the rule, and since the certification is for a purpose that is not “treatment, payment or operations”, the provider will need to get an authorization to release the certification to the employer. But the obligation to get the authorization is on the provider, and not the employer in this case.

There is an important exception to this rule. If the employer wants access to information about the employee seeking an ADA accommodation held in its Group Health Plan files, then the employer will need to first secure the employee’s authorization. This is consistent with the general application of the Privacy Rules, under which the Group Health Plan must secure an authorization before disclosing information for purposes other than treatment, payment or health care operations.

Because the ADA has some of its own privacy protections, compliance with both the ADA and HIPAA involves some subtle nuances. Under applicable EEOC guidance, an employer may not have access to an employee’s entire medical file, even for purposes of establishing that the employee’s condition does not pose a threat to health or safety, unless it first establishes that the entire file is necessary. EEOC rules describe at length what documentation is adequate for ADA purposes and what is not. And once medical information is provided to the employer, the employer must keep it in files that are separate from the employee’s general personnel file, and to which only a limited number of employees have access. Since HIPAA does not apply to this information, it should also be kept apart from the Group Health Plan files.

b) Family and Medical Leave Act (“FMLA”)

Employers also require medical information to determine whether an employee has a “serious health condition” that qualifies him or her for FMLA leave. The DOL has prescribed a medical certification form for this purpose that is filled out by a provider and submitted to the employer. As is the case with ADA certifications, the physician that examines the employee and issues the FMLA certification will need to get the employee’s authorization, but the information that results is not PHI in the hands of the employer so long as it does not come from the employer’s Group Health Plan.

c) Disability Plans

Unlike the ADA and FMLA, which involve potential conflicts with other Federal laws, disability, paid medical leave and extended leave arrangements are not so burdened. But the basics of HIPAA compliance are not too different. The employer will in most instances require a medical opinion from a provider/covered entity subject to the Privacy Rule. And since the opinion is other than for treatment, payment or healthcare operations, the provider will need to get an authorization from the

employee. The exception that applies in the case of the ADA and FMLA applies here as well. If the employer wants access to information about the employee held in its Group Health Plan files, an authorization is necessary. The preamble to the final Privacy Rule makes clear on more than one occasion that an employer can condition the grant of a disability benefit upon receipt of a duly executed authorization form.

d) Workers' Compensation

The HIPAA Privacy Rules contain an exception for disclosures of PHI for workers' compensation purposes that allows a Covered Entity to make the disclosure without authorization when required under applicable state law.

e) On-Site Medical Clinics

On-site clinics are excluded from the definition of a health plan for HIPAA purposes. But the inquiry does not end here. If an on-site clinic is a covered provider—i.e., it engages in electronic transactions covered by the EDI rule—then it is a Covered Entity that is subject to the Privacy Rules.

f) Pre-Employment Physical Examinations

Pre-employment physicals are governed in a manner similar to that involving disability claims. This is classically an employer and not a Plan Sponsor function, so the Privacy Rules are not implicated. The provider that performs the examination will need to obtain an authorization to release the results to the employer.

g) Employee Assistance Plans ("EAPs")

Many, if not most, EAPs will be subject to the Privacy Rules. ERISA has for some time distinguished between "referral-only" EAPs (that were not subject to ERISA) and EAPs that actually provided counseling (that were subject to ERISA). Those EAPs that are covered by ERISA will automatically be subject to the Rules. But even some EAPs that are not subject to ERISA will nonetheless be subject to the Privacy Rules. Any EAP that provides access to counseling through a vendor (a/k/a business associate) is likely subject to the Privacy Rules. Where the employer itself operates the EAP—i.e., an employer staffed call-in or drop-in center—it appears to fit the definition of an on-site clinic. Therefore, so long as it does not engage in covered electronic transmissions, it will not be subject to regulation as a provider.

Where an EAP is subject to the Privacy Rules, the employer and the EAP will need to take special care with psychotherapy notes. Covered Entities must obtain authorizations for all disclosures of psychotherapy notes other than for use by the originator of the notes, for certain training purposes, to defend a legal action brought by the individual, or as otherwise expressly permitted by the Privacy Rules.

### **III. QUESTIONS AND ANSWERS RELATING TO THE NEW CLAIMS REVIEW REGULATIONS**

#### **A. Why are the DOL's new claims review regulations (the "Claims Regulations") important to my company?**

Your company should care about the new Claims Regulations because such Regulations impose administrative procedures that dramatically change the manner in which your company's Group Health Plan and, by extension, your company, handles claims for benefits under such Plan. Not complying with these procedures exposes your company to the risk of having its denial of benefits (or the denial of benefits of the insurer or HMO that it uses to provide coverage) overturned by a Federal court. In contrast, if your company complies with these procedures, it runs little risk of such an outcome (and the increased legal fees that accompany it).

#### **B. What general requirements for claims administration do the Claims Regulations impose?**

##### *1. Why did the DOL issue new claims review regulations for Group Health Plans?*

The DOL intended the new Claims Regulations to serve as a "poor man's" patient's bill of rights. In fact, the DOL delayed final implementation of the regulations for more than one year while Congress was considering adopting a patient's bill of rights. When it became clear that Congress was not going to adopt a patient's bill of rights, the DOL issued the regulations in final form. Suffice it to say that the Claims Regulations are intended to make it easier for participants in Group Health Plans to dispute claims for benefits that have been denied.

##### *2. What dramatic changes do the new Claims Regulations make to Group Health Plan administration?*

The new Claims Regulations make several major changes in the relationship between the participant and the Group Health Plan in which he or she participates. First, participants are entitled to much faster review of their claims for benefits. For example, claims for urgent care must be decided within 72 hours. Even routine claims for a medical benefit must be decided within 30 days. Second, the regulations require the participant to be provided with all relevant information relating to his or her claim, even including information that was not used to decide the claim. Third, in the case of any claim for benefits involving medical judgment, the plan must consult a medical professional with appropriate training. Fourth, in the case of any appeal of a denied claim, the employer must ensure that the individual deciding the appeal (1) is not the individual or a subordinate of the individual who originally decided the claim and (2) does not defer to the judgment of the individual who originally decided the claim. Fifth, in the

case of any appeal of a denied claim where medical judgment is an issue, the employer must ensure that a medical professional who is not the same person or a subordinate of the medical professional who decided the first claim must be consulted.

3. *What kinds of employer-sponsored plans are covered by the DOL Claims Regulations?*

Almost any employer-sponsored welfare plan is covered. Welfare plans include employer sponsored health, accident and medical plans. Also included are disability, life insurance, severance, employee assistance and training plans or programs. However the Claims Regulations have the most dramatic effect on employer-sponsored health, medical and disability programs.

4. *What are the basic responsibilities of my company under the new Claims Regulations?*

While the specific employer responsibilities depend on the type of plan and how it is funded, basically, the employer needs to do three things: 1) Make sure that its welfare plan documents incorporate all of the requirements of the new Claims Regulations; 2) Adequately communicate the provisions of the new Claims Regulations to its employees; and 3) Make sure that the party that determines claims follows the requirements of the new Claims Regulations.

**C. When is a Group Health Plan covered by the Claims Regulations? Is it my company's responsibility to comply with the Claims Regulations?**

1. *Are plans that are not sponsored by an employer covered?*

No. Only employer-sponsored plans are covered. Therefore, if an employee buys and pays for his own disability insurance, that plan is not covered by the Claims Regulations.

2. *Are life insurance plans and disability plans covered?*

Yes, if they are sponsored by the employer.

3. *What is the difference between a fully insured and a self-insured plan for purposes of claims administration?*

In a fully insured arrangement, the employer (Plan Sponsor) enters into a contract to provide health benefits. So long as the employer maintains the policy, it is the responsibility of the insurance carrier to pay benefits under the Plan. The insurance carrier is subject to the requirements of the state insurance laws of the states in which it does business. In the typical insured arrangement, the employer has no input or control over whether a claim for benefits is approved or denied.

In a non-insured or self-administered arrangement, the employer is responsible for paying all of the benefits payable under the Plan and it is the employer-appointed Plan Administrator that is responsible for approving and denying claims. It is common for employers in self-insured arrangements to purchase “stop loss” insurance to cover the possibility that claims may exceed expectations. In many arrangements, employers retain a third party to review claims, but it is not uncommon for the employer to retain final authority to approve or deny a claim.

4. *My company’s insurance carrier has total responsibility for maintaining and operating the Group Health Plan. Does my company need to get involved in the claims administration process?*

Yes. First, while the insurance carrier may be responsible for paying and deciding claims, your company, in its capacity as Plan Administrator, is responsible for ensuring that claims are processed in accordance with the Claims Regulations. Unless the insurance carrier is an official of your company’s Plan (which would be quite rare), the carrier will not be legally responsible for complying with such Regulations. Second, participants are likely to request your company’s assistance in appealing denied claims.

5. *Who is the Plan Administrator of my company’s Group Health Plan?*

The Plan Administrator is the individual or organization appointed by your company to administer the plan. If your company does not appoint a Plan Administrator, it will become the default Plan Administrator.

6. *Why isn’t my company’s insurance carrier the Plan Administrator of my company’s fully insured Group Health Plan? After all, the insurance carrier has “total responsibility” for operating the Plan.*

The insurance carrier really does not have total responsibility for operating the Plan. It is the company that decides what kind of plan to maintain, how generous the benefits should be and whether employees and beneficiaries have to contribute to the cost of the coverage. The company can decide to provide more generous benefits to certain groups, such as executives, and to provide different types of plans in different geographical areas.

7. *What are the responsibilities of the Plan Administrator of my company’s Group Health Plan?*

The Plan Administrator has the overall responsibility for operating the Plan. This responsibility includes filing forms with the DOL and the Internal Revenue Service, distributing a summary plan description to participants and beneficiaries, and ensuring that the Plan is operated in accordance with federal law.

8. *What are the responsibilities of the “claims administrator” of my company’s Group Health Plan?*

The Plan Administrator frequently enlists the assistance of its insurance carrier or some other third party in doing the bulk of work to administer claims in accordance with the new Claims Regulations. The person or entity so designated, or in the absent of a designation, the Plan Administrator, is what is known as the “Claims Administrator”.

The Claims Administrator exercises discretionary authority in the approval or denial of claims. Discretionary authority is the authority to exercise judgment based upon a set of facts and circumstances. For example, the authority to deny a claim for a medical procedure because the treatment is experimental is discretionary authority. Other than deciding claims, most Claims Administrators (who are not also Plan Administrators) have no other responsibilities under a Group Health Plan. Of course, insurers and HMOs have other contractual responsibilities to pay benefits.

9. *Who is the Claims Administrator of a Group Health Plan?*

The answer depends on whether the Plan is self-administered or administered by an insurance carrier or other third party. As noted above, in a fully insured plan, the insurance carrier typically administers the day-to-day operation of the plan and serves as the Claims Administrator. In a self-insured plan, the employer will serve as the Claims Administrator unless it contracts with a third party for the performance of claims administration functions.

10. *Who is responsible for ensuring that the requirements of the new Claims Regulations are followed by the Claims Administrator?*

The Plan Administrator is responsible. Even though the insurance carrier in an insured Plan is responsible for approving and denying claims, its responsibilities under most employers’ medical plans do not include compliance with the new Claims Regulations. In the case of a self-insured plan that is third-party administered, the Claims Administrator typically will be an insurance carrier or similar organization with claims review experience.

11. *Why hasn’t my company’s insurance carrier told me about the requirements imposed on my company by the new Claims Regulations?*

This is really a question for your company’s insurance carrier. We can only speculate about its reasoning. In general, insurance carriers are concerned with selling policies and collecting premiums. Anything that complicates this process makes it less profitable, and the insurance carriers don’t want to complicate things unless absolutely necessary. Also, insurance carriers are directly regulated by the state insurance departments in the

states that they do business. They are not directly subject to the requirements of ERISA. Because ERISA and its claims procedures ultimately are the responsibilities of the Plan Administrator, most insurance carriers don't want to get involved. Another reason is that in the past the DOL did not actively enforce compliance with required claims procedures, and employers would suffer no penalties if they failed to comply with DOL procedures.

12. *Can't my company just appoint the insurance carrier to serve as the Plan Administrator?*

It's a good idea, but chances are that the insurance carrier won't want the job.

Even though most insurance carriers are willing to sell policies that provide medical benefits, it is rare that an insurance carrier is willing to take on the total responsibility of administering a medical plan. Most insurers will take responsibility for deciding claims, but they don't want the job of administering an employer's entire "benefit plan". For instance, only the employer can decide which classes of employees should participate, or how much to charge employees for beneficiary coverage.

13. *What has changed to make it so important that my company start complying with the new Claims Regulations?*

Several things. First, the new Claims Regulations impose substantive requirements upon Group Health Plans and Plan Administrators, creating rights that participants will be more likely to enforce. Second, the DOL has announced that it intends to vigorously enforce compliance with the new Claims Regulations. Third, Group Health Plans and Plan Administrators that do not follow these Regulations may have to litigate claims in federal court, and will lose the deferential standard of review normally granted to a Plan's administrative decisions. Ultimately, Plans that lose the deferential standard of review will end up paying higher claims.

14. *What are the risks to my company if it does not monitor the Claims Administrator to ensure compliance with the new Claims Regulations?*

The greatest risk is that the participant will have the right to litigate his or her claim in federal court without having to go through the Plan's claims procedures. Also, the participant may complain to the DOL, likely triggering an audit of the plan. Any employer who has undergone such an audit knows that it is an event to be avoided.

15. *Couldn't a participant always sue for benefits in federal court?*

Generally, no. Under ERISA, the courts generally have required a participant to have his or her claim decided by the Plan and "exhaust" all administrative review procedures under the Plan before bringing legal action. Even when legal action was commenced, the participant would prevail only if the Plan's decision was "arbitrary and capricious"

(unreasonable). Also, any federal court proceedings would be decided solely on the basis of the “administrative record.”

16. *What is an administrative record?*

An administrative record is a record of the proceedings before the Plan. For example, if a participant files a claim for benefits for a medical procedure and the insurance carrier denies the claim on behalf of the Plan, because it deems the procedure experimental, the participant’s claim and the insurance carrier’s denial are part of the administrative record. If the participant appeals the claim and submits a letter from his or her doctor, and the insurance carrier reviews the doctor’s letter and denies the appeal, because it disagrees with the doctor, the doctor’s letter, the participant’s appeal letter and the insurance carrier’s denial letter are part of the administrative record.

17. *Why was it disadvantageous for a participant to litigate claims for benefits in federal court before the new Claims Regulations took effect?*

Under the example in the previous question, a participant could not introduce new evidence in federal court. The court would decide his or her claim based solely on his or her claim and the doctor’s letter that he or she submitted. In addition, the courts generally denied participants the right to find out more about the basis for the insurance carrier’s position. Because the only role of the federal court was to review the Plan’s previous decision, most courts decided that participants had no rights to additional discovery.

In the past, insurance carriers used court decisions to their advantage. It was (and still is) common for insurance carriers to deny claims without providing detailed explanations of the reasons for the denial and without providing copies of plan documents, medical evidence, or internal procedures relied upon in making its decision. Many participants who disputed the insurance carrier’s decision wrongly assumed that they would be able to obtain insurance company documents in federal court.

As is discussed in detail below, all of this has changed under the new Claims Regulations.

18. *What does it mean for the court to defer to the administrative decision of the Plan?*

When a court “defers” to the administrative decision of a Plan, it will not overturn that decision, even if it would have decided the claim differently. Only in the case where the decision was so unreasonable that no reasonable person would have reached the Plan’s decision, will the court overturn the decision.

19. *What will happen to the cost of the Plan if claims are decided without deference to the decision of the Plan?*

The short answer is that the plan will have to pay more claims and larger claims and costs will rise. Under the new Claims Regulations, if the participant does not receive all of the information required under the Regulations and have his or her claim decided in a timely manner, the participant will no longer be subject to the “administrative exhaustion” requirement and will be able to go directly to federal court.

20. *What should my company do to make sure that my insurance carrier follows the new Claims Regulations?*

In the first instance, your company should ask its insurance carrier how it intends to comply with the new Claims Regulations and insist that the insurance carrier provide details. Some insurance carriers have decided that they can best serve their policy holders by helping them to fully comply with the Claims Regulations. Others continue to ignore the regulations, essentially taking the position that it is the responsibility of the Plan Administrator to comply. To be prudent, your company, in its capacity as Plan Administrator of its Group Health Plan, should ask its insurance carrier to provide copies of its internal procedures for complying with the new Claims Regulations. These procedures should include, for example, protocols for ensuring that claims for similarly situated participants are decided in the same manner, and procedures for selecting medical professionals to decide claims.

21. *What should my company do if the insurance carrier refuses to follow the new Claims Regulations?*

This presents a difficult practical problem. While it is not the insurance carrier’s responsibility to comply with the new Claims Regulations, most carriers should know that their insurance products are designed to be used in connection with employee benefit plans covered by ERISA and any product that they sell should be designed to comply with the requirements of ERISA, including the new Claims Regulations. If the carrier continues to refuse to comply with the Regulations, the best approach is to work with the carrier and to convince it that that Plan has a legal obligation to comply. One way of convincing the insurance carrier that it must comply with the new Claims Regulations is to offer to request an advisory opinion from the DOL as to the adequacy of the Plan’s procedures. In the final analysis, however, the Plan should not be in the position of purchasing insurance from a carrier that refuses to follow the provisions of applicable law.

**D. How quickly must a claim for benefits under my company's Group Health Plan be decided?**

1. *How quickly must a claim for benefits be decided?*

That depends on the type of claim. A claim for benefits under a Group Health Plan falls into one of four categories: 1) Urgent Care Claim; 2) Pre-Service Claim; 3) Post-Service Claim; and 4) Concurrent Care Claim.

2. *What is an Urgent Care Claim?*

An Urgent Care Claim is any claim for medical care or treatment that the treating physician believes could seriously jeopardize the life or health of the insured or subject the insured to severe pain that cannot be adequately managed unless the care or treatment is approved. This type of claim generally includes those situations commonly treated as emergencies.

3. *How quickly must an Urgent Care Claim be decided?*

In general, an Urgent Care Claim must be decided within 72 hours.

4. *What is a Pre-Service Claim?*

A Pre-Service Claim is a claim for a benefit under the Group Health Plan with respect to which the terms of the Plan require approval (usually referred to as pre-certification) of the benefit in advance of obtaining medical care.

5. *How quickly must a Pre-Service Claim be decided?*

In general, a Pre- Service Claim must be decided within 15 days.

6. *What is a Concurrent Care Claim?*

A Concurrent Care Claim is a claim regarding the termination of a previously approved course of treatments or an extension of the duration or number of treatments provided through a previously-approved benefit claim.

7. *How quickly must a Concurrent Care Claim be decided?*

That depends on the type of Concurrent Care Claim. If the claim involves the termination or curtailment of a course of previously approved treatments, any such termination or curtailment is treated as an "adverse claim decision" and any such decision must be made so that the participant or beneficiary has sufficient time to appeal the adverse decision and receive a decision on such appeal before the end of the course of treatments. For example, if a plan approves a course of physical therapy treatments

over the course of 6 months, and it subsequently wants to limit those treatments to 5 months, it would have to advise the participant or beneficiary at least 3 months in advance of the end of the 5 month period, so that the participant or beneficiary has 60 days to file an appeal, and the Plan would then have 30 days to decide the appeal. A claim for extension of a course of previously approved treatments involving Urgent Care must be decided within 24 hours.

8. *What is a Post-Service Claim?*

A Post-Service Claim is a claim for a benefit under the Plan that is neither a Pre-Service Claim nor a Concurrent Care Claim. This type of claim includes a request for reimbursement for medical services that have been billed to a participant by his or her medical provider and a request for an insurance carrier or HMO to cover health care services that have already been provided.

9. *How quickly must a Post-Service Claim be decided?*

In general, a Post-Service Claim must be decided within 30 days. This period may be extended one time for up to 15 days, provided that the Claims Administrator both determines that such an extension is necessary due to matters beyond the control of the plan and notifies the participant or beneficiary, prior to the expiration of the initial 30-day period, of the circumstances requiring the extension of time and the date by which a decision can be expected.

**E. What information must be provided to a participant or *beneficiary* who has made a claim for benefits under my company's Group Health Plan?**

1. *Who is entitled to make a claim for benefits under my company's Group Health Plan?*

Any participant or beneficiary for whom a benefit is available under the terms of the Group Health Plan may make a claim for such benefit.

2. *What happens if a participant or beneficiary does not provide enough information for the claim to be decided?*

The Plan Administrator/Claims Administrator may ask for an extension of time to decide the claim for benefits. If such an extension is necessary, the Plan Administrator/Claims Administrator must send the participant or beneficiary a notice of extension, specifically describing the information that the participant or beneficiary must submit to have the claim decided. The participant or beneficiary must be afforded at least 45 days from receipt of the notice within which to provide the specified information.

3. *What information must be provided to a participant or beneficiary upon denial of a claim for benefits under my company's Group Health Plan?*

- a) the specific reason or reasons for the adverse determination;
- b) reference to the specific Plan provisions on which the determination is based;
- c) a description of any additional material or information necessary for the participant or beneficiary to perfect the claim and an explanation of why such material or information is necessary;
- d) a description of the Plan's review procedures and the time limits applicable to such procedures, including a statement of the participant's or beneficiary's right to bring legal action in federal court;
- e) a copy of any internal rule, guideline, protocol, or other similar criterion that was relied upon in making the adverse determination, or a statement that a copy of any such rule, guideline, protocol or other similar criterion will be provided free of charge upon request;
- f) if the adverse benefit determination is based on a medical necessity or experimental treatment or similar exclusion or limit, an explanation of the scientific or clinical judgment used in the determination, applying the terms of the plan to the claimant's medical circumstances, or a statement that such explanation will be provided free of charge upon request; and
- g) in the case of an adverse benefit determination by a Group Health Plan concerning an Urgent Care Claim, a description of the expedited review process applicable to such a claim. This description may be provided to the claimant orally, provided that a written or electronic notification is furnished to the claimant not later than 3 days after the oral notification.

4. *What other information regarding a participant or beneficiary's claim for benefits must be provided to the participant or beneficiary upon request?*

A copy of any document that is relevant to the claim. A document is considered "relevant" if such document:

- a) was relied upon in making the benefit determination;
- b) was submitted, considered, or generated in the course of making the benefit determination, whether or not it was relied upon in making the benefit determination;

- c) demonstrates compliance with the administrative procedures and safeguards required under the Claims Regulations; or
- d) is a statement of policy or guidance concerning the denied treatment option or benefit for the claimant's diagnosis, without regard to whether such advice or statement was relied upon in making the benefit determination.

5. *Does this mean that certain information is considered relevant even if it was not used to decide the claim under appeal?*

Yes, any document that was submitted, considered or generated in the course of deciding the claim, or that constitutes an administrative safeguard or statement of policy, is considered relevant and must be disclosed. This is true even if the insurance carrier claims that the document contains proprietary information.

6. *Why does the requirement to disclose relevant information represent such a drastic change in the way claims are administered?*

Under ERISA, a court generally will not overturn an insurer's decision unless the claimant can prove that such decision was "arbitrary and capricious." Under the old regulations, it was extremely difficult for a participant or beneficiary making a claim to obtain information about the internal decision-making process of the insurer with respect to his or her claim. Without such information, it was difficult for the typical participant or beneficiary to prove that the insurer made an arbitrary and capricious decision.

Under the new Claims Regulations, a participant or beneficiary has a right to obtain all "relevant" information, thereby giving him or her greater ability to challenge the insurer's decision. More importantly, if the insurer does not provide the information, the participant or beneficiary can sue the employer and the insurer in federal court, essentially asking the federal court to decide the claim. Plan Sponsors now need to be especially careful in ensuring that their insurance carriers comply with the new Claims Regulations. Otherwise, they run the risk of having the claims denial decisions challenged in federal court, and having the court decide the claims without the protection of the arbitrary and capricious standard.

7. *Are there any other rules that must be followed in the claims administration process?*

Yes. A Group Health Plan may not adopt or administer claims review procedures in a way that unduly inhibits the initiation or processing of claims for benefits. Requiring payment of a fee to initiate a claim for benefits or to appeal a denied claim clearly is prohibited.

A Group Health Plan may not preclude an authorized representative of a claimant from acting on behalf of such claimant in pursuing a benefit claim or appeal of an adverse benefit determination.

The claims procedures must contain administrative processes and safeguards designed to ensure and to verify that claims are decided in accordance with plan documents and that procedures are applied consistently with respect to similarly situated claimants.

**F. What appeal rights does a participant or beneficiary have with respect to a denied claim for benefits under my company's Group Health Plan?**

1. *Do the new Claims Regulations give participants and beneficiaries extensive and greater appeal rights?*

Yes. The new Claims Regulations require that any appeal process be "reasonable." Despite what many insurers and employers may think, this is not an easy requirement to satisfy.

2. *What general requirements apply to a "reasonable" appeals procedure?*

An appeals procedure for a Group Health Plan is not reasonable unless it provides the following:

- a) provides a participant or beneficiary with at least 180 days within which to appeal an adverse determination;
- b) provides for a review that does not afford deference to the initial adverse benefit determination and that is conducted by a named fiduciary of the Plan who is neither the individual who made the initial determination, nor a subordinate of such individual;
- c) provides that, in deciding an appeal of any adverse benefit determination that is based in whole or in part on a medical judgment, including a determination with regard to whether a particular treatment, drug, or other item is experimental, investigational, or not medically necessary or appropriate, the decision maker shall consult with a health care professional who has appropriate training and experience in the field of medicine involved in the medical judgment;
- d) provides for the identification of medical or vocational experts whose advice was obtained on behalf of the plan in connection with a claimant's initial determination, without regard to whether the advice was relied upon in making the benefit determination;

- e) provides that the health care professional engaged for purposes of a consultation in connection with the appeal shall be an individual who is neither an individual who was consulted in connection with the initial benefit determination that is the subject of the appeal, nor the subordinate of any such individual; and
- f) provides, in the case of an Urgent Care Claim, for an expedited review process pursuant to which—
  - (1) a request for an expedited appeal of an adverse benefit determination may be submitted orally or in writing by the participant or beneficiary; and
  - (2) all necessary information, including the Plan's benefit determination on review, shall be transmitted between the Plan and the claimant by telephone, facsimile, or other available similarly expeditious method.

3. *How quickly must an appeal of a denied Urgent Care Claim be decided?*

In general, such an appeal must be decided within 72 hours after the Claims Administrator receives it.

4. *How quickly must an appeal of a denied Pre-Service Claim be decided?*

In general, such an appeal must be decided within 30 days from the date on which the Claims Administrator receives it.

5. *How quickly must an appeal of a denied Post-Service Claim be decided?*

In general, such an appeal must be decided within 60 days from the date on which the Claims Administrator receives it.

6. *How quickly must an appeal of a denied Concurrent Care Claim be decided?*

In general, such an appeal must be decided within 72 hours after receipt if the claim also qualifies as an Urgent Care Claim. Otherwise, such an appeal generally must be decided before the benefit is reduced or terminated.

7. *What information must be provided to a participant or beneficiary upon denial of his or her appeal?*

The participant or beneficiary must be provided with written (or, if certain requirements are met, electronic) notification of the following:

- a) the specific reason or reasons for the denial;

- b) reference to the specific Plan provisions on which the denial is based;
  - c) a statement that the participant or beneficiary is entitled to receive, upon request and free of charge, reasonable access to, and copies of, all documents, records, and other information relevant to the claimant's claim for benefits.
  - d) if an internal rule, guideline or protocol was relied upon, either a copy of the specific rule, guideline or protocol, or a statement that a copy of the rule, guideline, or protocol was relied upon and will be provided free of charge to the participant or beneficiary upon request;
  - e) if the denial is based on a medical necessity or experimental treatment or similar exclusion or limit, either an explanation of the scientific or clinical judgment for the determination, applying the terms of the Plan to the participant's or beneficiary's medical circumstances, or a statement that such explanation will be provided free of charge upon request; and
  - f) the following statement: "You and your Plan may have other voluntary alternative dispute resolution options, such as mediation. One way to find out what may be available is to contact your local U.S. Department of Labor Office and your State insurance regulatory agency."
8. *How many levels of appeal may my company's Group Health Plan require a participant or beneficiary to undergo before he or she may bring a law suit?*

The Plan may require no more than two levels of appeal.

9. *May my company's Group Health Plan require that a participant or beneficiary arbitrate his or her claim for benefits?*

Yes. However, the arbitration requirement may not interfere with the participant's or beneficiary's right to bring a claim for benefits in Federal or State court.

10. *What rights does a participant or beneficiary have if his or her appeal is denied?*

The participant or beneficiary has a right to bring a law suit in Federal or State court under ERISA to overturn the decision of the Plan. He or she may also have the right to participate in any procedure established under the applicable state insurance law for review of the decision of the insurer or HMO.

#### **IV. QUESTIONS AND ANSWERS RELATING TO GROUP HEALTH PLAN DOCUMENT, SUMMARY PLAN DESCRIPTION AND DOCUMENT DISCLOSURE REQUIREMENTS**

##### **A. What “plan document” requirements apply to my company’s Group Health Plan?**

1. *What documentation is my company required to have with respect to its Group Health Plan?*

ERISA requires your company to maintain both a Plan document and a summary plan description.

2. *What is a plan document ?*

A Plan document is a legal document that specifies all aspects of the operation and administration of a Plan.

3. *What information must be contained in the Plan document for my company’s Group Health Plan?*

The Plan document must contain all of the requirements and rules with respect to the operation of the Plan, including, but not limited to, exactly who is covered by the Plan, and how much each participant or beneficiary must pay toward the cost of the coverage. The Plan document also must contain all of the pertinent rules that govern the operation of the Plan, including the parties responsible for its operation and administration, and rules governing denial of claims. Finally, if the Plan or your company, as Plan Sponsor, uses PHI, the Plan document must contain various rules restricting and regulating the use of such information.

4. *Must my company’s Group Health Plan be in writing?*

Yes. ERISA requires that every employer-sponsored Group Health Plan be established and maintained pursuant to a written plan document.

5. *May the terms of my company’s Group Health Plan be contained in more than one document?*

Yes, ERISA specifically permits a Plan to be operated in accordance with one or more written documents. As long as each one of the documents is clearly identified as part of the Plan, several documents may constitute part of a single Plan.

6. *What is meant by the phrase “documents under which the plan is operated”?*

ERISA requires that a Plan be “operated” in accordance with one or more written instruments. Although one of these documents may be labeled as a “plan” document,

other documents may also govern the operation of the Plan and, therefore, may be relevant to a Plan participant or beneficiary seeking to determine his or her benefits. The Plan Administrator is required to provide a participant or beneficiary receiving benefits under the Plan all of the documents under which the Plan is operated upon request.

7. *How does an insurance policy differ from a Plan document for a Group Health Plan?*

An insurance policy is an agreement between an insurance carrier and an employer to provide certain benefits to the employer's employees upon payment of certain premiums. To the extent that an insurance policy describes benefits payable to participants it may constitute one of the "documents under which the plan is operated".

8. *Why is the insurance policy for my company's Group Health Plan not a sufficient plan document?*

Because an insurance policy does not contain all of the necessary provisions that need to be contained in a Plan, such as the classes of employees that are eligible to participate, the rules for operating the Plan, who is responsible for making decisions under the Plan, and the parties responsible for amending and/or terminating the Plan.

9. *Why hasn't my company's insurance carrier told me that my company needs a Plan document for the Group Health Plan?*

Because insurance carriers do not practice law and it is not their responsibility to advise employers about the scope and extent of employers' legal responsibilities under ERISA. Most insurance carriers view their sole responsibility as fulfilling the requirements of their contract with the sponsor of the Plan.

10. *But my company's insurance carrier and its representatives are experts. Don't they realize that my company relies on their advice regarding what it needs to do to comply with the law?*

There is no easy answer to this question. The contract or insurance policy between the Plan Sponsor and the insurer rarely obligates the insurer to provide authoritative advice to the Plan Sponsor regarding its legal obligations. However, it is not uncommon for brokers and agents, as part of their sales pitches, to encourage, or at least not dispel, the belief that Plan Sponsors can rely upon such industry expertise.

11. *Is there another compelling reason to write a separate Plan document?*

Yes. DHHS recently issued privacy regulations concerning the use or disclosure of PHI by a Group Health Plan. With limited exceptions, any Plan that has access to any PHI

must set forth written procedures concerning the use or disclosure of PHI in the plan document.

12. *When must a Plan document be provided to a plan participant or beneficiary?*

A Plan Administrator is not required to provide the Plan document unless requested by the participant or beneficiary. However, if the terms of the Plan are set forth in more than one document, all of the documents under which the Plan is operated must be provided.

13. *Must the Plan document be provided free of charge?*

In general, no. The Plan Administrator may impose a reasonable copying charge to provide the Plan document. However, if the Plan document is requested as part of the claims review process, it must be provided free of charge.

14. *How long does the Plan Administrator have to provide the plan document?*

Under ERISA, the Plan Administrator has 30 days from the date of the request, unless the delay is caused by a reason beyond the control of the Plan Administrator.

15. *What happens if the Plan Administrator does not provide the Plan document within 30 days?*

The Plan Administrator may become liable for a penalty of up to \$110 per day (the exact amount to be decided by the court, in its sole discretion) for each day that the Plan document is not provided.

16. *What should my company do if it never has written a Plan document for its Group Health Plan and a participant or beneficiary requests one?*

The employer should write a Plan document as soon as possible. A plan administrator that provides an insurance policy or group insurance certificate as a substitute for a Plan document runs the risk of being hit with the \$110 penalty described above and civil litigation.

**B. What are the new content requirements applicable to a summary plan description for a Group Health Plan?**

1. *What is a summary plan description ?*

A summary plan description, or “SPD,” is a layman’s description of a Plan that is required to be distributed under the requirements of ERISA and DOL regulations.

2. *In general, what information is required to be contained in the summary plan description for my company's Group Health Plan?*

In general, an SPD for a Group Health Plan must accurately describe the material provisions of the plan in layman's terms. For example, a well-drafted SPD should describe, among other items, all of the benefits provided under the Plan, the Plan's eligibility requirements, the portion the cost of benefits that must be borne by the participant or beneficiary, any deductible and coinsurance requirements that may apply, the circumstances which would result in a loss of benefits, procedures for making benefit claims and appealing adverse decisions and the persons responsible for administration and operation of the Plan.

3. *What other specific information must be contained in an SPD?*

DOL regulations specify numerous specific items that must be incorporated into the SPD, such as the name and address of the Plan Sponsor and the Plan Administrator and a description of COBRA rights and other legal rights applicable to participants in Group Health Plans. The SPD is also required to contain language describing each participant's ERISA rights, using model language provided by the DOL.

4. *May the SPD for my company's Group Health Plan be contained in more than one document?*

Yes, the information may be set forth in more than one document as long as each document clearly provides that the required information is contained in two or more documents.

5. *Who is responsible for providing a summary plan description to the participants or beneficiaries of my company's Group Health Plan?*

By law, the Plan Administrator is responsible for drafting and distributing an SPD to participants and beneficiaries. It is not the responsibility of the insurance carrier or the HMO to draft an SPD or distribute it to participants or beneficiaries.

6. *What is a group insurance "certificate of coverage"?*

A group insurance certificate of coverage, or Group Insurance Certificate, is a summary of the benefits provided under a policy of insurance that is generally filed with the insurance department of the state in which the policy is written. The Group Insurance Certificate is generally distributed to participants and beneficiaries in the form of a booklet describing the benefits provided by the insurance policy.

7. *Why can't the Group Insurance Certificate prepared by my company's insurance carrier also serve as the SPD for my company's Group Health Plan?*

Because the SPD is required to contain information that generally is not contained in the Group Insurance Certificate. An SPD that does not contain this information does not comply with DOL regulations.

8. *What additional information needs to be contained in the summary plan description?*

Generally, an insurance company-drafted Group Insurance Certificate does not contain information concerning the classes of employees eligible to join the Plan, the cost of the Plan to the employee, a description of the Plan's claims procedures, and a description of who is responsible for amending or terminating the Plan.

9. *The Group Insurance Certificate for my company's Group Health Plan contains a two-page attachment entitled Summary Plan Description. Can the Group Insurance Certificate and the two-page attachment serve as an SPD?*

Probably not. It is rare for an insurance company-drafted attachment to fulfill all of the stringent requirements imposed by DOL regulations. Most do not contain the information described in Question 8 above.

10. *What is the risk to my company of using an insurance company-drafted document as an SPD?*

Any employer that fails to draft a summary plan description that complies with the regulations risks audit by the DOL. If the SPD does not comply with DOL regulations, the Plan Administrator risks that a court will deem the SPD deficient and impose a \$110 per day penalty for failure to distribute an SPD. If the SPD does not establish adequate claims procedures, participants and beneficiaries may have the right to bypass the Plan's claims procedures and bring a claim for benefits directly in federal or state court.

11. *Do the DOL's new Claims Regulations have to be included in the summary plan description?*

Generally, yes. The claims procedures are an important provision of the Plan, and they must be communicated to participants and beneficiaries. Although a Plan Administrator has the option of writing a separate claims administration document, the better approach, one taken by the vast majority of Plan Administrators, is to incorporate the claims procedures into the SPD. DOL regulations contain a specific requirement that the claims procedures be communicated to participants and beneficiaries. Most Plan Administrators choose to do so through the SPD.

12. *Do the Plan's HIPAA Privacy Rule compliance procedures have to be included in the summary plan description?*

Yes. Any Group Health Plan that has access to PHI or permits the employer, in its capacity as Plan Sponsor or Plan Administrator, to have access to PHI must contain rules restricting access to such PHI. These rules constitute a material feature of the Plan that must be reflected in the SPD.

13. *When must a summary plan description be distributed to participants?*

In general, the SPD must be distributed within 120 days after the later of the date on which the plan is adopted or made effective. New enrollees generally must receive an SPD within 90 days after commencing participation in the Plan.

14. *What is the risk to my company of failing to comply with the SPD regulations?*

The Plan Administrator generally is required to distribute an SPD to a participant or beneficiary within 90 days after the commencement of participation. Further, the plan administrator must provide an SPD to any participant or beneficiary who requests one. Failure to provide an SPD subjects the Plan Administrator of a penalty of up to \$110 per day for each day that the failure continues.

15. *My company's group insurance booklets are prepared by the insurance carrier. What should my company do if the insurance carrier refuses to change or enhance the information provided to participants and beneficiaries?*

This question presents a difficult problem. Most employers select an insurance carrier or HMO based upon the cost of insurance benefits. One way an insurer can save costs is to minimize the amount of time and resources it devotes to legal compliance. However, if the insurer refuses to agree to include legally required language (such as a discussion of claims procedures) in an SPD because it does not intend to follow the applicable regulations, the Plan Administrator may become liable for penalties for failure to distribute an SPD, as a defective SPD would not suffice. The employer's benefit costs could rise, as the Plan could become liable to pay benefits that it otherwise would not have to pay (i.e., if communicated a legally sufficient claims procedure to its participants and beneficiaries). In the final analysis, the employer, in its role as Plan Sponsor of its Group Health Plan, must weigh the cost of failing to comply with the regulations against the cost savings that may be achieved by continuing to use a carrier that refuses to comply with all of its legal requirements.

16. *Why doesn't my company's insurance carrier take responsibility to do everything that needs to be done for my company's Group Health Plan?*

Essentially, this is a question that your insurance carrier should answer. However, the simple answer is that up until now market forces have not forced insurance carriers to comply with DOL and ERISA regulations. This has placed the responsibility for writing and distributing a summary plan description squarely on the employer and the Plan Administrator. Therefore, unless a significant number of Plan Administrators demand that insurers provide adequate SPDs and Plan documents, the insurers will continue to have no incentive to do so.

**C. What additional disclosure requirements apply to Plan documents and summary plan descriptions for Group Health Plans?**

1. *What other documents may have to be disclosed to a participant or beneficiary upon request?*

There are two classes of documents that must be disclosed to a participant or beneficiary. The first class of documents relates to the operation of the Plan itself. These include, in addition to the plan document and the SPD:

- a) 1) all other instruments under which the plan is operated, such as any underlying insurance policies; and 2) the Plan's annual report (IRS Form 5500). These documents must be disclosed by the Plan Administrator within the 30 days after any participant or beneficiary requests them. A reasonable charge can be imposed for copying these documents. However, no charge may be imposed if the request is made in connection with a claim for benefits.
- b) The second class of documents that must be disclosed relate to a participant's or beneficiary's claim for benefits. These documents must be disclosed upon the request of a participant or beneficiary if his or her claim for benefits has been denied. These documents include, but are not limited to: 1) all documents relied upon by the Claims Administrator to decide the claim, including internal insurance company protocols; and 2) all documents relevant to the claim whether or not relied upon by the Claims Administrator (any document generated in the course of reviewing the claim is considered relevant).

2. *How quickly must documents be disclosed if requested by a participant or beneficiary?*

Documents that are required to be disclosed under ERISA generally must be disclosed within 30 days of request. Documents that are required to be disclosed to participants or beneficiaries in connection with the claims process must be disclosed when a claim or

appeal is denied, or within a reasonable time after such documents are requested by the participant or beneficiary.

3. *Is it the responsibility of the Plan Administrator or the insurance carrier to provide summary plan descriptions, Plan documents, government filings or other instruments under which the Plan is operated to the participant or beneficiary?*

ERISA places this responsibility squarely upon the Plan Administrator.

## **V. CONCLUSION AND PRACTICAL CONSIDERATIONS**

As demonstrated by the length and complexity of this booklet, the scope of most companies' legal obligations with respect to their Group Health Plans has been increased dramatically by the new Privacy Rules and Claims Regulations. Because the scope of these rules as applied to employers is not widely known throughout the professional community, many employers continue to be confused or misinformed about their new legal obligations under the Privacy Rules and Claims Regulations.

Employers are reacting to this confusion and complexity in a number of ways. Understandably, many employers are reacting by doing as little as possible to comply with the new requirements, assuming that the cost of compliance will exceed the penalties and other liabilities that could result from the failure to comply. Other employers intend to rely upon advice given by so-called HIPAA experts (which is incorrect) that they do not need to have access to PHI if they maintain a fully insured medical plan. An employer taking this approach loses the ability to assist employees with disputed claims and the ability to monitor whether its insurer or HMO has complied with the Claims Regulations. Still other employers would like to comply with the new Privacy Rules and Claims Regulations, but do not know exactly what needs to be done (and what can be done) given their budgetary constraints.

While the extent of the enforcement activities that will be undertaken by the governmental agencies that oversee the Privacy Rules and the Claims Regulations is not entirely known at this early date, it is clear that the most severe penalties will be reserved for those employers that do nothing to meet their legal obligations. On the other hand, employers that can demonstrate that they have made a good faith effort to meet their legal obligations are likely to be treated less harshly by the courts and regulatory agencies.

In recognition of all of these factors, the Employee Benefits Practice Group at Brown Rudnick Berlack Israels LLP has designed an affordable compliance package that will enable most employers that sponsor fully insured medical plans to fulfill most of their compliance obligations at an affordable, fixed cost.

The compliance package consists of:

- 1) a "wrap around" plan document and a "wrap around" SPD, both of which are designed to be used in conjunction with the insurance company-provided documents and plan descriptions;
- 2) a compliance manual containing many of the typical forms that would be used in connection with administration of the Privacy Rules; and
- 3) a one-day training session for personnel who may have access to PHI on key aspects of the Privacy Rules.

Employers desiring additional information should contact any one of the attorneys in Brown Rudnick Berlack Israels' Employee Benefits Practice Group listed below:

|                            |               |                       |
|----------------------------|---------------|-----------------------|
| Harvey M. Katz             | 212-209-4860  | hkatz@brbilaw.com     |
| George L. Chimento         | 617- 856-8503 | gchimento@brbilaw.com |
| James L. Hauser            | 617-856-8130  | jhauser@brbilaw.com   |
| Adam B. Cantor             | 212-209-4896  | acantor@brbilaw.com   |
| Pamela L. Kearse           | 617-856-8164  | pkearse@brbilaw.com   |
| Rita L. Gelman (Paralegal) | 212-209-4838  | rgelman@brbilaw.com   |

**GLOSSARY OF TERMS**

|  |  |
|--|--|
| <b>ADA</b>   | Americans with Disabilities Act of 1990, as amended.   |
| <b>Administrative Services Only (ASO)</b>              | A contract with an insurance company or other third party to provide administrative services to a self-insured medical plan.   |
| <b>Adverse Benefit Determination</b>                   | Denial, reduction, or termination of, or a failure to provide or make payment (in whole or in part) for, a benefit, including decisions as a result of (i) ineligibility to participate in a plan; (ii) application of any utilization review; or (iii) because the benefit is determined to be experimental or not medically necessary. |
| <b>Authorization</b>                                   | Written permission from an individual that gives a Covered Entity or employer permission to use or disclose Protected Health Information (or other confidential medical information) for specified purposes, which are generally purposes other than managing treatment, payment, or health care operations.                             |
| <b>Business Associate</b>                              | A person or service provider that performs or assists a Covered Entity with activities involving the use or disclosure of Protected Health Information.  |
| <b>Claim for Benefits</b>                              | A request for benefits under a Group Health Plan made by a Participant or Beneficiary in accordance with the Group Health Plan's reasonable procedures for filing benefit claims.  |
| <b>Claims Administrator</b>                            | An insurance carrier, HMO or some other third party appointed by a Plan Administrator to exercise discretionary authority over the approval or denial of claims.   |
| <b>Claim Denial</b>                                    | See " <i>Adverse Benefit Determination</i> "   |
| <b>Claims Regulations or Claims Denial Regulations</b> | Regulations, promulgated under ERISA by the DOL, governing procedures that must be utilized by a Group Health Plan when a claim for benefits is denied.  |
| <b>COBRA</b>   | Health care continuation requirements of the Consolidated Omnibus Budget Reconciliation Act of 1986.   |
| <b>Concurrent Care Claim</b>                           | A claim regarding the termination of a previously approved course of treatments or an extension of the duration or number of treatments provided through a previously-approved benefit claim.  |

|   |  |
|---|--|
| <b>Consent</b>                          | Written permission, which a Covered Entity has the option of obtaining from an individual, to use or disclose protected health information for the purpose of facilitating treatment of an individual, payment of claims, or healthcare operations.  |
| <b>Covered Entity</b>                   | A healthcare provider that engages in the electronic transmission of confidential health information, a Group Health Plan, or a healthcare clearinghouse.  |
| <b>De-Identified Health Information</b> | Protected Health Information that is stripped of all identifying data so as to prevent someone from recognizing the individual who is the subject of the information.  |
| <b>Designated Record Sets</b>           | A group of records maintained by or for a Covered Entity that includes (i) medical and billing records; (ii) records relating to enrollment, payment, and claims; (iii) case or medical management records maintained by or for the Group Health Plan; or (iv) any record used in whole or in part to by a covered entity to make decisions about individuals. |
| <b>DHHS</b>                             | United States Department of Health and Human Services.   |
| <b>DOL</b>                              | United States Department of Labor.   |
| <b>ERISA</b>                            | Employee Retirement Income Security Act of 1974, as amended.   |
| <b>Fiduciary</b>                        | Any person or organization that exercises discretionary authority over the administration or assets of a Group Health Plan or who has authority to do so. Both the Plan Administrator and the Claims Administrator are Fiduciaries under ERISA by virtue of their respective areas of discretionary authority.   |
| <b>FMLA</b>                             | Family and Medical Leave Act of 1993, as amended.  |
| <b>Fully-Insured Plan</b>               | A Group Health Plan arrangement where, by contract, the employer is responsible for maintaining and paying premiums under the insurance policy or HMO contract, but has no input or control over whether a claim for benefits is approved or denied, and an insurance carrier or HMO is responsible for paying benefits under the Group Health Plan.           |

|                                   |  |
|-----------------------------------|--|
| <b>Group Health Plan</b>          | A benefit plan or program maintained by an employer that provides medical care, including items and services paid for as medical care to employees and/or their dependents through insurance, reimbursement or otherwise.                              |
| <b>Group Insurance Booklet</b>    | Generally, a booklet prepared by an insurance carrier or HMO describing the benefits payable under an insurance policy or contract with an HMO.  |
| <b>Health Care Operations</b>     | Activities relating to general administrative and business functions necessary for a Group Health Plan to conduct its business.  |
| <b>HIPAA</b>                      | Health Insurance Portability and Accountability Act of 1996, as amended.   |
| <b>HMO</b>                        | Health Maintenance Organization.   |
| <b>Minimum Necessary Standard</b> | A standard contained in the Privacy Rules requiring a Covered Entity to limit disclosure of Protected Health Information to the minimum information necessary to satisfy an inquiry received by the Covered Entity.                                    |
| <b>Payment</b>                    | Tasks relating to core functions through which health care and health insurance services are funded such as, eligibility or coverage determinations, claims review, utilization review, coordination of benefits and medical necessity determinations. |
| <b>PHI</b>                        | Protected Health Information, or confidential medical information that is individually identifiable.   |
| <b>Plan Administrator</b>         | Person or organization appointed by an employer who has the authority and responsibility to manage and direct the operation and administration of a Group Health Plan, or if no person or organization is appointed, the employer itself.              |
| <b>Plan Document</b>              | Written document or documents required under ERISA, that establishes and governs the administration of a Group Health Plan.  |
| <b>Plan Sponsor</b>               | An employer, when acting in its role of implementing, or adopting, amending, terminating or funding a Group Health Plan.   |

|                                   |  |
|-----------------------------------|--|
| <b>Post-Service Claim</b>         | A request for reimbursement for medical services that have been billed to a participant by his or her medical provider and a request for any insurance carrier or HMO to cover health care services that have already been provided.   |
| <b>Pre-Service Claim</b>          | A claim for a benefit under the Group Health Plan with respect to which the terms of the plan require approval (usually referred to as a pre-certification) of the claim in advance of obtaining medical care.   |
| <b>Privacy Official</b>           | An individual designated by his or her employer to be responsible for maintaining policies and procedures that ensure the employer's compliance with HIPAA.  |
| <b>Privacy Rules</b>              | Privacy rules that apply to Protected Health Information under regulations promulgated under HIPAA by DHHS.  |
| <b>Relevant Document</b>          | Any document that was (i) relied upon by a Claims Administrator in making an adverse benefit determination; (ii) was submitted, considered or generated in the course of making a benefit determination even if not relied upon; (iii) demonstrates compliance with the administrative procedures and safeguards required under the Claims Regulations; and (iv) is a statement of policy or guidance concerning the denied treatment option or benefit for the clients' diagnosis, without regard to whether such advice or statement was relied upon in denying the claim. |
| <b>Self-Administered Plan</b>     | A plan for which the employer serves as Plan Administrator both in name and in the actual performance of day to day management of the plan.  |
| <b>Self-Insured Plan</b>          | A group health plan in which all payments for coverage are made by the employer directly from its general assets or from a trust funded by the employer. It is customary for an employer to protect itself against the possibility of catastrophic losses under this type of arrangement through purchase of "stop-loss" insurance.  |
| <b>Summary Health Information</b> | Health information, which may be PHI, that i) has been cleansed of most of its individually identifiable characteristics and ii) in the aggregate, summarizes the claims history, claims expenses, or types of claims experienced by individuals covered under the employers Group Health Plan.  |

|   |  |
|---|--|
| <b>Summary Plan Description</b>                           | A layman's description of the relevant provisions of a Group Health Plan that is required to be distributed to participants and beneficiaries under the requirements of ERISA and DOL regulations, often referred to by its abbreviation "SPD".  |
| <b>Treatment</b>  | Those tasks relating to the provision, coordination and management of health care.   |
| <b>Treatment, Payment or Health Care Operations (TPO)</b> | Core health care functions for which protected health information (or confidential medical information) may be used or disclosed by a Covered Entity without permission or authorization from an individual. The Privacy Rules include a blanket exception, often called the "TPO" exception, for such uses and disclosures to facilitate activities relating to the provision of health care services by health care providers, payment for such services by insurance companies or other parties responsible for paying an individual's medical bills, and management of health insurance programs by Plan Sponsors. |
| <b>Urgent Care Claim</b>                                  | Any claim for medical care or treatment that the treating physician believes could seriously jeopardize the life or health of the participant or subject the participant to severe pain that cannot be adequately managed unless the care or treatment is approved.  |

## INDEX

### A

ADA: *See* Americans with Disabilities Act  
 administrative exhaustion, 39 (III.C.15), 41 (III.C.19)  
 administrative record, 40 (III.C.16)  
 administrative services only, 9 (II.C.9), 59 (glossary)  
 adverse benefit determination, 44 (III.E.3, 4), 59 (glossary)  
 Americans with Disabilities Act, 14 (II.C.26), 32-33 (II.G.2), 59 (glossary)  
 appeal rights of participant, 46-48 (III.F)  
 appeals procedure, general requirements, 46-47 (III.F.2)  
 appeals procedure, restrictions on levels of appeal, 48 (III.F.8)  
 appeals procedure, time requirements, 47 (III.F.3-6)  
 arbitration, 48 (III.F.9)  
 ASO: *See* administrative services only  
 authorization, 14 (II.C.27, 28), 17 (II.D.1), 18 (II.D.3), 26-27 (II.E.3), 30-31 (II.E.13), 33-34 (II.G.2), 59 (glossary)  
 authorization vs. consent, 26-27 (II.E.3)  
 authorization, circumstances when required, 26-27 (II.E.3)  
 authorization, participation in Group Health Plan conditioned on, 30 (II.E.13)  
 authorization, required elements, 26 (II.E.3)

### B

business associate, 17 (II.D.1), 18-19 (II.D.4), 31 (II.F.1), 34 (II.G.2), 59 (glossary)  
 business associate contract, 24 (II.D.17)  
 business associate, compliance standards for, 19 (II.D.4)  
 business associate, examples of functions and activities, 19 (II.D.4)

business associate, obligations to protect PHI, 18-19 (II.D.4), 23-24 (II.D.17)

business associate, subject to Privacy Rules, 17 (II.D.1), 18 (II.D.4), 34 (II.G.2)

### C

changes in new Claims Regulations, 35-36 (III.B.2), 39 (III.C.13), 40 (III.C.17), 41 (III.C.19), 45 (III.E.6), 46 (III.F.1)  
 claim denial: *See* adverse benefit determination  
 claim for benefits, 12 (II.C.22), 35-36 (III.A; III.B.2), 40 (III.C.16, 17), 42-48 (III.D; III.E; III.F), 59 (glossary)  
 claim for benefits, parties entitled to make claim, 43 (III.E.1)  
 claim for benefits, time requirements, 42-43 (III.D.1, 3, 5, 7, 9)  
 claim for benefits, types of claims, 42-43 (III.D.2, 4, 6, 8)  
 claims administrator, 38 (III.C.8, 9), 59 (glossary)  
 Claims Regulations, 12 (II.C.21, 22), 35-48 (III), 59 (glossary)  
 Claims Regulations, general requirements for claims administration, 35 (III.B.1-4)  
 Claims Regulations, inclusion in summary plan description, 53 (IV.B.11)  
 Claims Regulations, information to be provided to participant, 44-45 (III.E.3, 4), 47-48 (III.F.7)  
 Claims Regulations, intent of new regulations, 35 (III.B.1)  
 Claims Regulations, other requirements for claims administration, 45-46 (III.E.7)  
 Claims Regulations, participant's right to sue in federal court, 39-40 (III.C.14, 15, 17), 41 (III.C.19), 44 (III.E.3), 45 (III.E.6), 48 (III.F.9, 10)  
 Claims Regulations, participant's right to sue in state court, 48 (III.F.9, 10)

Claims Regulations, types of plans subject to, 10 (II.C.11), 36 (III.B.3; III.C.1, 2)

Claims Review Regulations: See Claims Regulations

COBRA, 52 (IV.B.3), 59 (glossary)

compliance with Claims Regulations, 35 (III.A), 38-39 (III.C.10, 11, 13, 14), 41 (III.C.20, 21)

compliance with Privacy Rules, 3 (II.A.1), 4 (II.A.5, 6), 6 (II.B.8), 10 (II.C.11, 12), 12-13 (II.C.20, 22, 23), 14 (II.C.28), 20-21 (II.D.7, 8), 23 (II.D.14, 15), 33 (II.G.2)

concurrent care claim, 42-43 (III.D.6, 7), 47 (III.F.6), 59 (glossary)

confidential medical information, 4 (II.A.5; II.B.1, 2), 6 (II.B.9), 11 (II.C.15), 14 (II.C.27), 61 (glossary)

consent, 17 (II.D.1), 18 (II.D.3), 26-27 (II.E.3), 60 (glossary)

consent vs. authorization, 26-27 (II.E.3)

Consolidated Omnibus Budget Reconciliation Act: See COBRA

court's deference to administrative decision of the plan, 39 (III.C.13), 40-41 (III.C.18, 19)

covered entity, 3 (II.A.2, 3), 4-5 (II.B.1, 2), 9 (II.C.10), 10 (II.C.11), 13 (II.C.23), 14 (II.C.29), 17 (II.D.1), 19 (II.D.4), 20 (II.D.8), 25 (II.E.1), 26 (II.E.3), 33-34 (II.G.2), 60 (glossary)

covered entity, Group Health Plan as, 3 (II.A.2, 3), 5 (II.B.2), 9 (II.C.10), 13 (II.C.23)

## D

deadline for implementation of Privacy Rules, 20 (II.D.7)

de-identified health information, 6 (II.B.9), 11 (II.C.15), 60 (glossary)

denial of appeal, information to be provided to participant, 47-48 (III.F.7)

denial of claim, information to be provided to participant, 44-45 (III.E.3, 4)

Department of Health and Human Services: See DHHS

Department of Labor: See DOL

designated record sets, 29 (II.E.9), 60 (glossary)

DHHS, 1 (I), 4 (II.A.6; II.B.1), 21 (II.D.8), 31 (II.F.2, 3), 32 (II.G.2), 50 (IV.A.11), 60 (glossary)

disability plans, 33-34 (II.G.2), 36 (III.B.3; III.C.2)

disclosure of PHI, about deceased individual, 28 (II.E.6)

disclosure of PHI, accidental, 24 (II.D.18)

disclosure of PHI, basic principles, 17-18 (II.D.1)

disclosure of PHI, incidental, 24 (II.D.18)

disclosure of PHI, to personal representative, 27-28 (II.E.4, 6)

disclosure of PHI, to personal representative of unemancipated minor, 28 (II.E.4, 5)

disclosure of PHI, to plan administrator, 21 (II.D.10)

disclosure of PHI, to plan sponsor, 21 (II.D.10)

disclosure, additional requirements for Group Health Plan documentation, 55 (IV.C.1-3)

dis-enrollment information, 10 (II.C.13), 12 (II.C.18-20), 17 (II.D.1)

DOL, 1 (I), 4 (II.A.5), 12 (II.C.22), 33 (II.G.2), 35 (III.A; III.B.1), 37 (III.C.7), 39 (III.C.11), 41 (III.C.21), 51 (IV.B.1), 52 (IV.B.3), 53 (IV.B.7, 9-11), 55 (IV.B.16), 60 (glossary)

## E

EAP: See employee assistance plan

employee assistance plan, 34 (II.G.2)

Employee Retirement Income Security Act: See ERISA

employer access to PHI, 6 (II.B.7), 12 (II.C.19, 21), 14 (II.C.26), 54 (IV.B.12)

employer involvement in claims process, 12 (II.C.21)

employer responsibilities re. Claims Regulations, 36 (III.B.4), 37 (III.C.4), 41 (III.C.20)

employer responsibilities re. Group Health Plan documentation, 50 (IV.A.9), 54 (IV.B.15), 55 (IV.B.16)

employer responsibilities re. Privacy Rules, 3 (II.A.1, 2, 4), 10 (II.C.11, 12), 13 (II.C.23, 24), 14 (II.C.26, 27), 23 (II.D.15), 24-31 (II.E.1-13)

employer responsibilities re. Privacy Rules and service providers, 23-24 (II.D.17)

employer's administrative obligations handling PHI, 22-23 (II.D.13)

employer-sponsored welfare plan, 36 (III.B.3)

employment record, 14 (II.C.27)

enrollment information, 10 (II.C.13), 12 (II.C.18-20), 17 (II.D.1)

ERISA, 1 (I), 4 (II.A.5), 9 (II.C.9), 10 (II.C.11), 12 (II.C.22), 13 (II.C.24), 20 (II.D.5, 6), 30 (II.E.10), 34 (II.G.2), 39 (III.C.11, 15), 41 (III.C.21), 45 (III.E.6), 48 (III.F.10), 49 (IV.A.1, 4-6), 50 (IV.A.9), 51 (IV.A.14; IV.B.1), 52 (IV.B.3), 55 (IV.B.16; IV.C.2), 56 (IV.C.3), 60 (glossary)

exemption from Privacy Rules, 3 (II.A.2), 10 (II.C.13), 11 (II.C.14)

## F

Family and Medical Leave Act, 14 (II.C.26), 33 (II.G.2), 60 (glossary)

federal employment laws and employment-related arrangements, interaction with Privacy Rules, 32-34 (II.G.2)

federal laws and Privacy Rules compliance, 14 (II.C.26, 28), 20 (II.D.6)

fiduciary, 4 (II.A.5), 10 (II.C.11), 13 (II.C.22), 46 (III.F.2), 60 (glossary)

fire wall requirements, 21 (II.D.9)

FMLA: See Family and Medical Leave Act

fully insured Group Health Plan, 4 (II.A.5), 6 (II.B.7), 7 (II.C.2), 8 (II.C.3, 6), 9 (II.C.7), 10 (II.C.11, 13), 11 (II.C.16), 12-13 (II.C.20-22), 15 (II.C.30), 17 (II.D.1), 36 (III.C.3), 37 (III.C.6), 38 (III.C.9), 60 (glossary)

## G

Group Health Plan, definition, 5 (II.B.3), 61 (glossary)

Group Health Plan, documentation requirements, 49-56 (IV)

Group Health Plan, fully insured, 4 (II.A.5), 6 (II.B.7), 7 (II.C.2), 8 (II.C.3, 6), 9 (II.C.7), 10 (II.C.11, 13), 11 (II.C.16), 12-13 (II.C.20-22), 15 (II.C.30), 17 (II.D.1), 36 (III.C.3), 37 (III.C.6), 38 (III.C.9), 60 (glossary)

Group Health Plan, fully insured, definition of, 8 (II.C.3), 60 (glossary)

Group Health Plan, notice of privacy rights, 25 (II.E.1), 26 (II.E.2)

Group Health Plan, participant's rights, 24-31 (II.E)

Group Health Plan, self-administered, 8 (II.C.5, 6), 9 (II.C.7-9), 15 (II.C.30), 37 (III.C.3), 38 (III.C.9), 62 (glossary)

Group Health Plan, self-insured, 6 (II.B.7), 7 (II.C.2), 8 (II.C.4, 5), 9 (II.C.7), 10 (II.C.11), 11 (II.C.14, 16), 15 (II.C.30), 36-37 (III.C.3), 38 (III.C.9, 10), 62 (glossary)

Group Health Plan, self-insured vs. self-administered, 8 (II.C.5)

Group Health Plan, subject to Privacy Rules, 7 (II.C.1), 8 (II.C.5-7), 9 (II.C.10), 10 (II.C.11), 12 (II.C.20), 13 (II.C.23), 14 (II.C.27)

Group Health Plan, types subject to Privacy Rules, 5 (II.B.4)

group insurance booklet, 54 (IV.B.15), 61 (glossary)

group insurance certificate, 51 (IV.A.16), 52 (IV.B.6), 53 (IV.B.7-9)

group insurance certificate, vs. summary plan description, 53 (IV.B.7-9)

## H

health care operations, definition, 18 (II.D.2), 61 (glossary)

Health Insurance Portability and Accountability Act: See HIPAA

health maintenance organization: See HMO

HIPAA, 1 (I), 3-34 (II), 61 (glossary)  
 HIPAA Privacy Rules: See Privacy Rules  
 HMO, 5 (II.B.3, 4), 8 (II.C.3, 6), 9 (II.C.9, 10), 10 (II.C.11, 13), 12 (II.C.21), 13 (II.C.22), 35 (III.A), 38 (III.C.8), 43 (III.D.8), 48 (III.F.10), 52 (IV.B.5), 54 (IV.B.15), 61 (glossary)

## I

individually identifiable health information, 5 (II.B.5), 6 (II.B.8), 61 (glossary)  
 insurance carrier, 4 (II.A.5), 5 (II.B.3, 4), 8 (II.C.3, 4, 6), 9 (II.C.9, 10), 10 (II.C.11), 22 (II.D.12), 36 (III.C.3), 37 (III.C.4, 6), 38-39 (III.C.8-12), 40 (III.C.16, 17), 41 (III.C.20, 21), 43 (III.D.8), 45 (III.E.5, 6), 50 (IV.A.7, 9, 10)  
 insurance carrier, responsibilities of, 3 (II.A.4), 36 (III.C.3), 37 (III.C.4, 6), 50 (IV.A.9), 52 (IV.B.5), 54 (IV.B.15), 55 (IV.B.16), 56 (IV.C.3)  
 insurance coverage, adopting, 13 (II.C.25)  
 insurance coverage, amending, 10 (II.C.12), 11 (II.C.16), 12 (II.C.20), 13 (II.C.25), 21 (II.D.10), 50 (IV.A.8), 53 (IV.B.8)  
 insurance coverage, re-bidding, 4 (II.A.5), 10 (II.C.12), 11 (II.C.16, 17), 13 (II.C.23, 25), 21 (II.D.10)  
 insurance coverage, terminating, 10 (II.C.12), 13 (II.C.25), 21 (II.D.10), 50 (IV.A.8), 53 (IV.B.8)  
 insurance policy, vs. plan document, 50 (IV.A.7, 8), 51 (IV.A.16)  
 intent of new Claims Regulations, 35 (III.B.1)  
 intent of Privacy Rules, 4-5 (II.B.2)

## M

marketing purposes, special handling of PHI, 17 (II.D.1), 27 (II.E.3)  
 minimum necessary standard, 14-15 (II.C.28, 29), 21 (II.D.11), 22 (II.D.12), 61 (glossary)

## N

noncompliance with Claims Regulations, risks of, 35 (III.A), 39 (III.C.13, 14), 41 (III.C.19), 45 (III.E.6)

noncompliance with documentation requirements, risks of, 51 (IV.A.15), 53 (IV.B.10), 54 (IV.B.14, 15)

noncompliance with Privacy Rules, penalties for, 31 (II.F.1)

noncompliance with Privacy Rules, risks of, 4 (II.A.6)

## O

on-site medical clinics, 32 (II.G.1), 34 (II.G.2)

## P

participant requests for amendments to PHI, 25 (II.E.1), 30 (II.E.10-12)  
 participant requests for confidential communication of PHI, 29 (II.E.8)  
 participant requests for restrictions on use or disclosure of PHI, 28 (II.E.7)  
 participant rights, Claims Regulations, 43-48 (III.E, III.F)  
 participant rights, Group Health Plan, 24-31 (II.E)  
 participant rights, Privacy Rules, private right of action, 31 (II.F.3)  
 participant's right to sue in federal court, Claims Regulations, 39-40 (III.C.14, 15, 17), 41 (III.C.19), 44 (III.E.3), 45 (III.E.6), 48 (III.F.9, 10)  
 participant's right to sue in state court, Claims Regulations, 48 (III.F.9, 10)  
 participation information, 10 (II.C.13), 12 (II.C.18-20), 17 (II.D.1)  
 payment, definition, 18 (II.D.2), 61 (glossary)  
 PHI, 5 (II.B.5), 61 (glossary)  
 PHI, business associate obligations to protect, 18-19 (II.D.4), 23-24 (II.D.17)  
 PHI, complaint process re. improper use/disclosure, 31 (II.F.3)  
 PHI, employer access to, 6 (II.B.7), 12 (II.C.19, 21), 14 (II.C.26), 54 (IV.B.12)  
 PHI, employer's "use or disclosure" obligations, 20-22 (II.D.8, 11, 12)  
 PHI, employer's administrative obligations, 22-23 (II.D.13)

- PHI, examples of, 5 (II.B.6)
  - PHI, need for access by fully insured plans, 12-13 (II.C.21, 22)
  - plan administrator responsibilities re.
    - Claims Regulations, 37 (III.C.7), 38 (III.C.10), 39 (III.C.11, 13), 41 (III.C.20)
  - plan administrator responsibilities re.
    - Group Health Plan documentation, 50 (IV.A.6), 51 (IV.A.12-16), 52 (IV.B.5), 54 (IV.B.14), 55 (IV.B.16), 56 (IV.C.3)
  - plan administrator responsibilities re.
    - Privacy Rules, 5 (II.B.2), 10 (II.C.11), 12 (II.C.22), 13 (II.C.24), 17-18 (II.D.1, 3), 20-22 (II.D.8, 11, 12), 24 (II.D.17)
  - plan administrator, definition, 37 (III.C.5), 61 (glossary)
  - plan document, definition and required elements, 49-50 (IV.A.2-8), 61 (glossary)
  - plan document, requirements for distribution, 51 (IV.A.12, 14, 15)
  - plan document, vs. insurance policy, 50 (IV.A.7, 8), 51 (IV.A.16)
  - plan sponsor responsibilities re. Privacy Rules, 5 (II.B.2), 10 (II.C.12), 13 (II.C.25), 14 (II.C.27), 20-21 (II.D.8, 10), 24 (II.D.17), 30 (II.E.13)
  - plan sponsor, definition, 13 (II.C.25), 61 (glossary)
  - post-service claim, 43 (III.D.8, 9), 47 (III.F.5), 62 (glossary)
  - pre-employment physical examinations, 34 (II.G.2)
  - pre-service claim, 42 (III.D.4, 5), 47 (III.F.4), 62 (glossary)
  - privacy official, 22 (II.D.13), 23 (II.D.14), 31 (II.F.3), 62 (glossary)
  - Privacy Rules, 3-34 (II), 62 (glossary)
  - Privacy Rules, application to employee benefit plans other than health plans, 32 (II.G.1)
  - Privacy Rules, application to employers, 3 (II.A.1, 2)
  - Privacy Rules, conditions when subject to, 7 (II.C.1), 8 (II.C.5, 6, 7), 9 (II.C.10), 10 (II.C.11), 13 (II.C.23), 14 (II.C.27)
  - Privacy Rules, deadline for implementation of, 20 (II.D.7)
  - Privacy Rules, definition, 4 (II.B.1), 62 (glossary)
  - Privacy Rules, employer training requirements, 23 (II.D.15)
  - Privacy Rules, exemption from, 3 (II.A.2), 10 (II.C.13), 11 (II.C.14)
  - Privacy Rules, federal agency responsible for enforcement, 1 (I), 31 (II.F.2)
  - Privacy Rules, inclusion in summary plan description, 54 (IV.B.12)
  - Privacy Rules, intent of, 4-5 (II.B.2)
  - Privacy Rules, participant's right to private action, 31 (II.F.3)
  - proprietary information, 45 (III.E.5)
  - Protected Health Information: See PHI
  - psychotherapy notes, special handling of PHI, 17 (II.D.1), 26-27 (II.E.3), 34 (II.G.2)
- R**
- relevant document, 44 (III.E.4), 45 (III.E.5), 62 (glossary)
  - required documentation, Group Health Plan, 49-50 (IV.A.1-6)
  - rights of Group Health Plan participants, 24-31 (II.E)
- S**
- self-administered Group Health Plan, 8 (II.C.5, 6), 9 (II.C.7-9), 15 (II.C.30), 37 (III.C.3), 38 (III.C.9), 62 (glossary)
  - self-insured Group Health Plan, 6 (II.B.7), 7 (II.C.2), 8 (II.C.4, 5), 9 (II.C.7), 10 (II.C.11), 11 (II.C.14, 16), 15 (II.C.30), 36-37 (III.C.3), 38 (III.C.9, 10), 62 (glossary)
  - self-insured Group Health Plan, vs. self-administered, 8 (II.C.5)
  - service provider obligations re. PHI, 18-19 (II.D.4), 23-24 (II.D.17)
  - SPD: See summary plan description
  - state laws and Privacy Rules compliance, 14 (II.C.26, 28), 18 (II.D.3), 19-20 (II.D.5), 28 (II.E.5), 30 (II.E.10), 31 (II.F.3), 34 (II.G.2)

summary health information, 10 (II.C.13),  
11 (II.C.15-17), 12 (II.C.20), 17 (II.D.1),  
21 (II.D.10), 62 (glossary)

summary health information vs. de-  
identified health information, 11 (II.C.15)

summary plan description, 1 (I), 37  
(III.C.7), 49 (IV.A.1), 51-55 (IV.B), 63  
(glossary)

summary plan description, disclosure  
requirements, 52 (IV.B.4, 5), 54 (IV.B.13)

summary plan description, required  
elements, 52 (IV.B.2, 3), 53 (IV.B.7-9,  
11), 54 (IV.B.12)

## **T**

TPO: See treatment, payment or health  
care operations

treatment, definition, 18 (II.D.2), 63  
(glossary)

treatment, payment or health care  
operations, 17 (II.D.1), 18 (II.D.2), 25  
(II.E.1), 26 (II.E.3), 28 (II.E.7), 33 (II.G.2),  
59 (glossary), 61 (glossary), 63  
(glossary)

treatment, payment or health care  
operations, definition, 18 (II.D.2), 63  
(glossary)

types of Group Health Plans subject to  
Privacy Rules, 5 (II.B.4)

types of plans subject to Claims  
Regulations, 10 (II.C.11), 36 (III.B.3;  
III.C.1, 2)

## **U**

urgent care claim, 42 (III.D.2, 3), 44  
(III.E.3), 47 (III.F.3), 63 (glossary)

## **W**

workers' compensation, 5 (II.B.4), 14  
(II.C.28), 15 (II.C.29), 32 (II.G.1), 34  
(II.G.2)

#### **About the authors:**

**Harvey M. Katz**, a partner at Brown Rudnick, is experienced in all aspects of pension and employee benefits law. His practice is diverse. He represents both plaintiffs and defendants in connection with benefit plan-related litigation, including claims denials, fiduciary responsibility, prohibited transactions, plan disqualification and tax-related issues. He also counsels clients about the employee benefits aspects of merger and acquisition and bankruptcy transactions. Mr. Katz is a leading expert in the emerging area of compliance with HIPAA privacy rules, which now restrict the use of confidential medical information in connection with medical plans. He is also consulted regarding the newly effective, stringent claims procedures that apply to all employer-sponsored medical, health, disability and similar plans. He frequently consults as an expert to other law firms with respect to such matters.

**James L. Hauser**, also a partner at Brown Rudnick, is experienced in advising clients on the design and administration of their health and welfare plans, qualified and non-qualified retirement plans, and stock option and stock purchase plans. He counsels companies on HIPAA compliance issues related to their group health plans and also represents clients with respect to a range of ERISA and executive compensation matters. Mr. Hauser has written and published numerous articles and frequently speaks on topics related to issues such as HIPAA and ERISA compliance, compensation and benefits programs.

**Adam B. Cantor**, a senior associate at Brown Rudnick, advises clients in all aspects of employee benefits law, including HIPAA and ERISA compliance; design, implementation and administration of pension, welfare and executive compensation plans; litigation strategies for benefit plan-related issues; transactional issues involved in mergers, acquisitions, bankruptcies and other major corporate events; tax planning and business succession planning. Mr. Cantor has written and published articles on such diverse topics as employee benefit issues in corporate downsizing, COBRA planning and compliance, and fiduciary liability under 401(k) plans.

#### **About the firm:**

**Brown Rudnick Berlack Israels LLP is a full-service, international law firm** with offices in the United States and Europe. Serving a global client base, the Firm's 200+ attorneys provide representation across key areas of the law: Corporate & Securities, Employee Benefits, Intellectual Property, Finance, Bankruptcy & Corporate Restructuring, Government Law & Strategies, Complex Litigation and Real Estate. Combining a dedication to excellence with an entrepreneurial spirit, we offer a breadth and depth of expertise uniquely suited to our clients' legal needs.

**Brown Rudnick Berlack Israels' Employee Benefits Practice Group** represents businesses at all stages of development, including emerging growth companies, public companies and large private institutional businesses. We provide a wide range of legal and consulting services to cover all aspects of employee benefits law, including compliance guidance and training, as well as design, implementation and administration of benefits plans and programs. In this complex area, we provide an aggressive, result-oriented approach to meeting the specific business goals of each client.

[www.brownrudnick.com](http://www.brownrudnick.com)



**BROWN  
RUDNICK  
BERLACK  
ISRAELS** LLP

One Financial Center  
Boston, MA 0211  
617.856.8200  
fax 617.856.8201

Alexandra House  
Ballsbridge, Dublin 4, IRL  
+353.1.664.1738  
fax +353.1.664.1838

CityPlace 1  
Hartford, CT 06103  
860.509.6500  
fax 860.509.6501

8 Clifford Street  
London, W1S 2LQ, UK  
+44.20.7851.6000  
fax +44.20.7851.6100

120 West 45th Street  
New York, NY 10036  
212.704.0100  
fax 212.704.0196

121 South Main Street  
Providence, RI 02903  
401.276.2600  
fax 401.276.2601

[www.brownrudnick.com](http://www.brownrudnick.com)